PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UNA EMPRESA INMOBILIARIA ALINEADO A LA NORMA ISO/IEC 27001:2013

ANEXOS

Zully Isabel Justino Salinas

ASESOR: Moisés Villena Aguilar

Lima, Febrero de 2015

CONTENIDO

ANEXO A. Política de Seguridad de Información

1. Definición:

La política de Seguridad de Información está formada por un conjunto de principios que la organización debe seguir para asegurar la confiabilidad de sus sistemas informáticos. Por sí misma, no constituye una garantía para la seguridad de información, se convertirá en una cuando responda a los intereses y necesidades de la empresa.

Este documento debe seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, tales como cambio en la infraestructura tecnológica, alta rotación de personal, desarrollo de nuevos servicios, entre otros.

Los principales beneficios de la implementación de la política son:

* Contribuir hacer efectiva la gestión del riesgo.
* Priorizar el valor de la información
* Estandarizar los controles y revisiones de los sistemas de información
* Establecer las bases para el desarrollo de estrategias y planes referidos a la seguridad de información.
* Cumplir con los requerimientos regulatorios y legales pertinentes.
* Brindar un entorno de trabajo seguro a los usuarios.

La entidad seguirá los lineamientos de la presente política de seguridad, así mismo se debe tener en cuenta que la seguridad de la información se caracteriza por la preservación de:

a) Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información;
b) Su integridad, asegurando que la información y sus métodos de proceso sean exactos y completos;
c) Su disponibilidad, asegurando que los usuarios tengan acceso a la información y a sus activos asociados cuando lo requieran.

2. Responsabilidad:

Es responsabilidad de la alta dirección conocer y hacer conocer los lineamientos de la Política de Seguridad de la información a todo el personal, de igual manera el personal es responsable de conocer y cumplir la Política de Seguridad de la Información, las normas relacionadas con ésta, los procedimientos y los estándares generales y aquellos específicamente relacionados con su área de competencia.

Dentro de este contexto, se puede diferenciar niveles de responsabilidad a través de las distintas funciones por parte del

- Área de administración:

  - Promover la difusión y apoyo a la seguridad de la información dentro de la organización y coordinar el proceso de administración de la continuidad de las actividades.

  - Tomar conocimiento y apoyar en el monitoreo de los incidentes relativos a la seguridad informática.

  - Aprobar las principales iniciativas para incrementar la seguridad de información, de acuerdo a las competencias y responsabilidades asignadas a cada área.

- Área de TI:

  - Minimizar la probabilidad de ocurrencia de incidentes a fin de mitigar el riesgo de errores derivados de estos.

  - Cubrir las necesidades de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnologías de las unidades de negocio.

  - Acordar y aprobar metodologías y procesos relativos a la seguridad de información.

  -Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

  - Coordinar las acciones del Comité de Seguridad de la información de impulsar la implementación de la presente política.

  - Monitorear aquellos cambios significativos derivados de los riesgos que afecten a los recursos informáticos.

- Capital Humano:

  - Notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la política de seguridad de la información y de todas las normas, procedimientos y prácticas que de ella surjan.

- Área legal:

  - Verificar el cumplimiento de la presente Política en lo relacionado a la gestión de los contratos, acuerdos u otra documentación de índole legal de la Organización con sus empleadores y terceros.

- Auditoría interna:

  - Desarrollar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, e informar el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta política y por las normas, procedimientos y prácticas que de ella surjan.

3. Política de Seguridad de la Información:

La información y sistemas de información tienen un valor importante para la organización, por lo que se deberá preservar su confidencialidad, integridad y disponibilidad para darle una efectiva protección a la información de manera que se equilibren los gastos utilizados en controles de seguridad de información contra los daños a la organización.

El objetivo de esta política es establecer lineamientos en la administración de la información con el fin de garantizar la seguridad de los sistemas que satisfaga el requerimiento del negocio y de mantener la integridad de la información, de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad. De esta manera la empresa se compromete en la formación y sensibilización del personal, contratistas y terceros involucrados, respecto a la seguridad de información para garantizar el cumplimiento de las normativas legales aplicables en busca de la seguridad de la información al interior y fuera de la organización.

4. Publicación y distribución:

La Política de Seguridad de la información debe ser comunicada a todos los usuarios de la organización, siendo de conocimiento y aplicación obligatorio para todo el personal de la entidad. Por parte de empresa, esta debe publicar y distribuir de forma adecuada hacia todos los niveles de la organización.

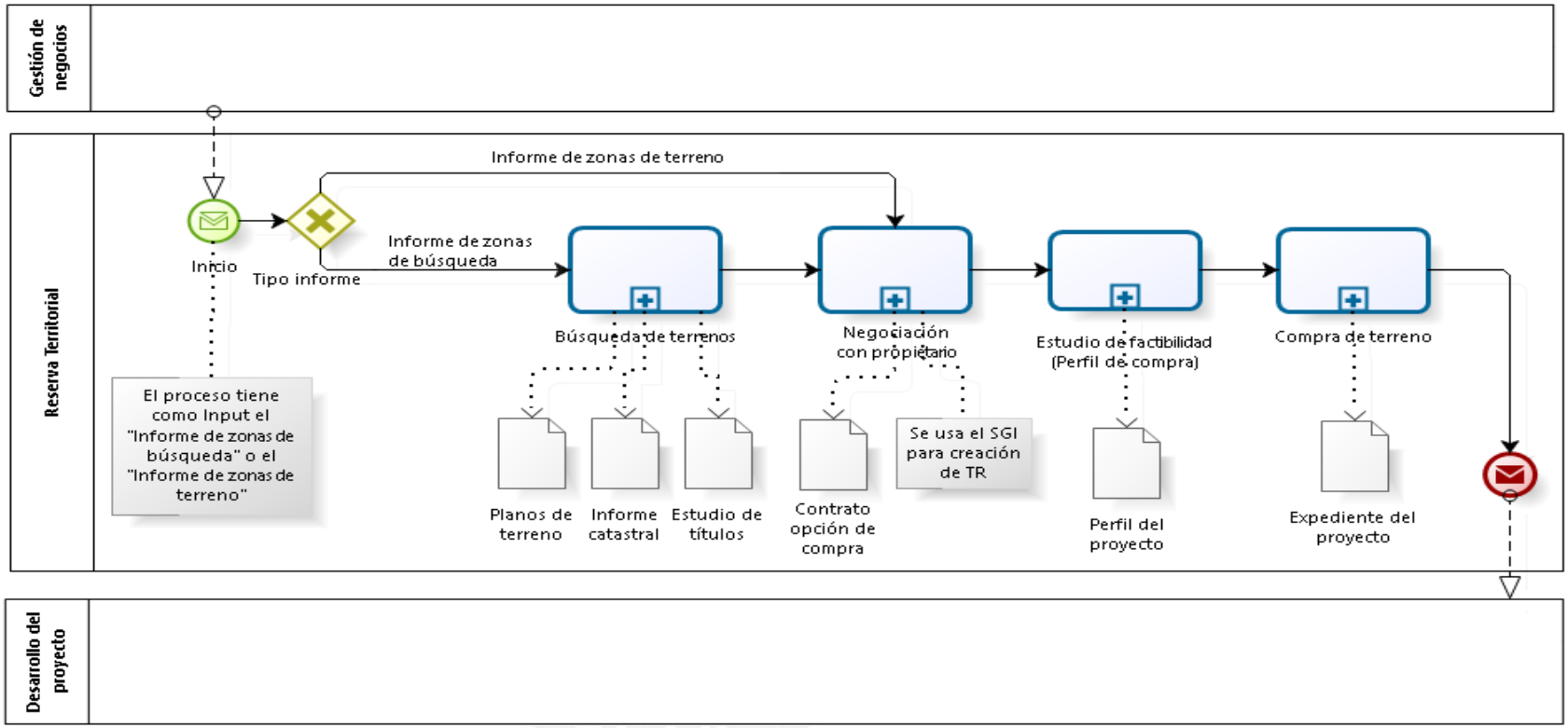
5. Incumplimiento:

A nivel interno, el incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones según el reglamento interno de trabajo (RIT). Las violaciones a la Política de seguridad de información y a cualquier procedimiento o pauta derivados de ésta, que ocasionen cualquier riesgo o pérdida directa para la organización pueden resultar en acción disciplinaria por parte de la organización cuya magnitud depende del tipo y severidad de la violación.

.

ANEXO B. Modelado de procesos en BPMN 2.0

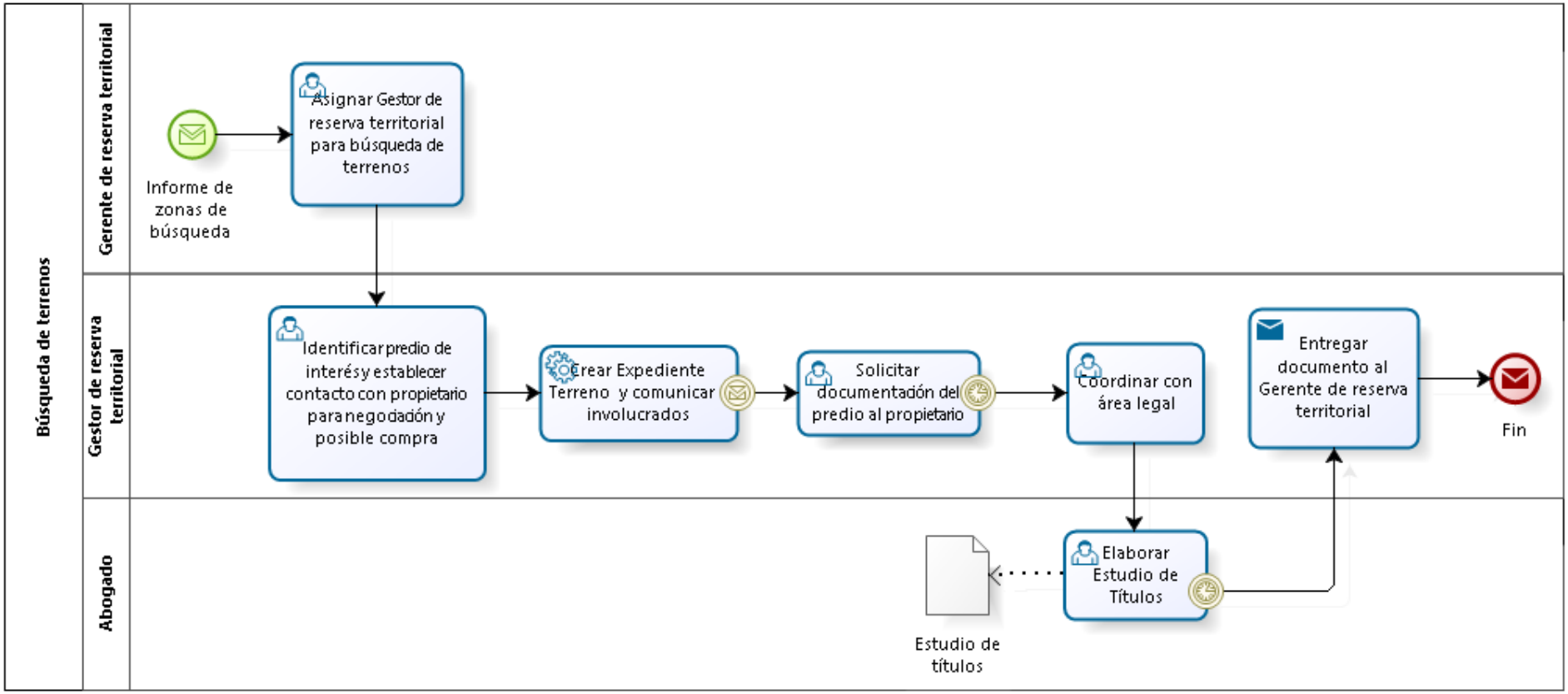
Anexo B.1 Macro-proceso Reserva Territorial



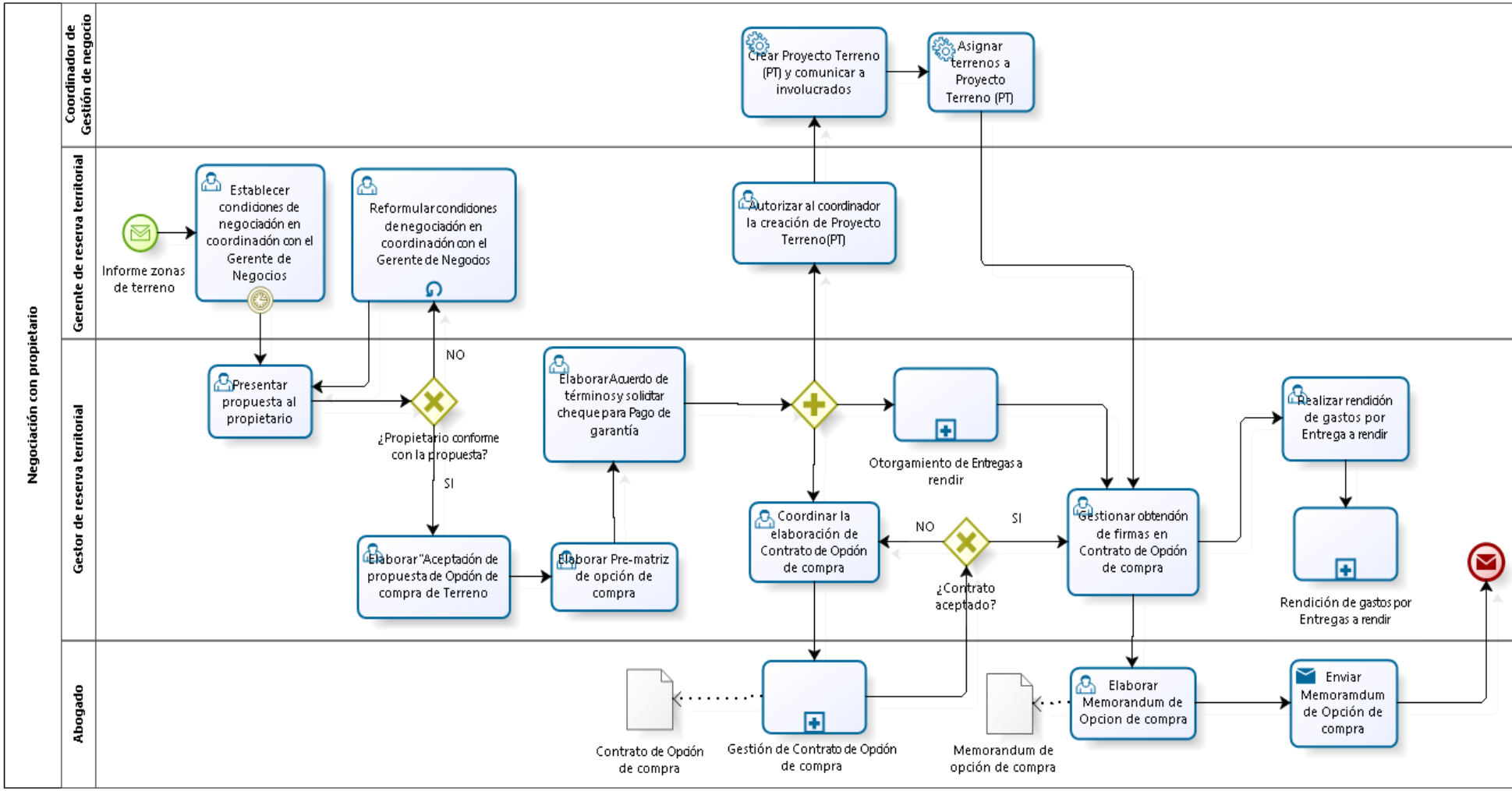
*

SGI, Sistema de Gestión Inmobiliario
TR, Expediente Terreno

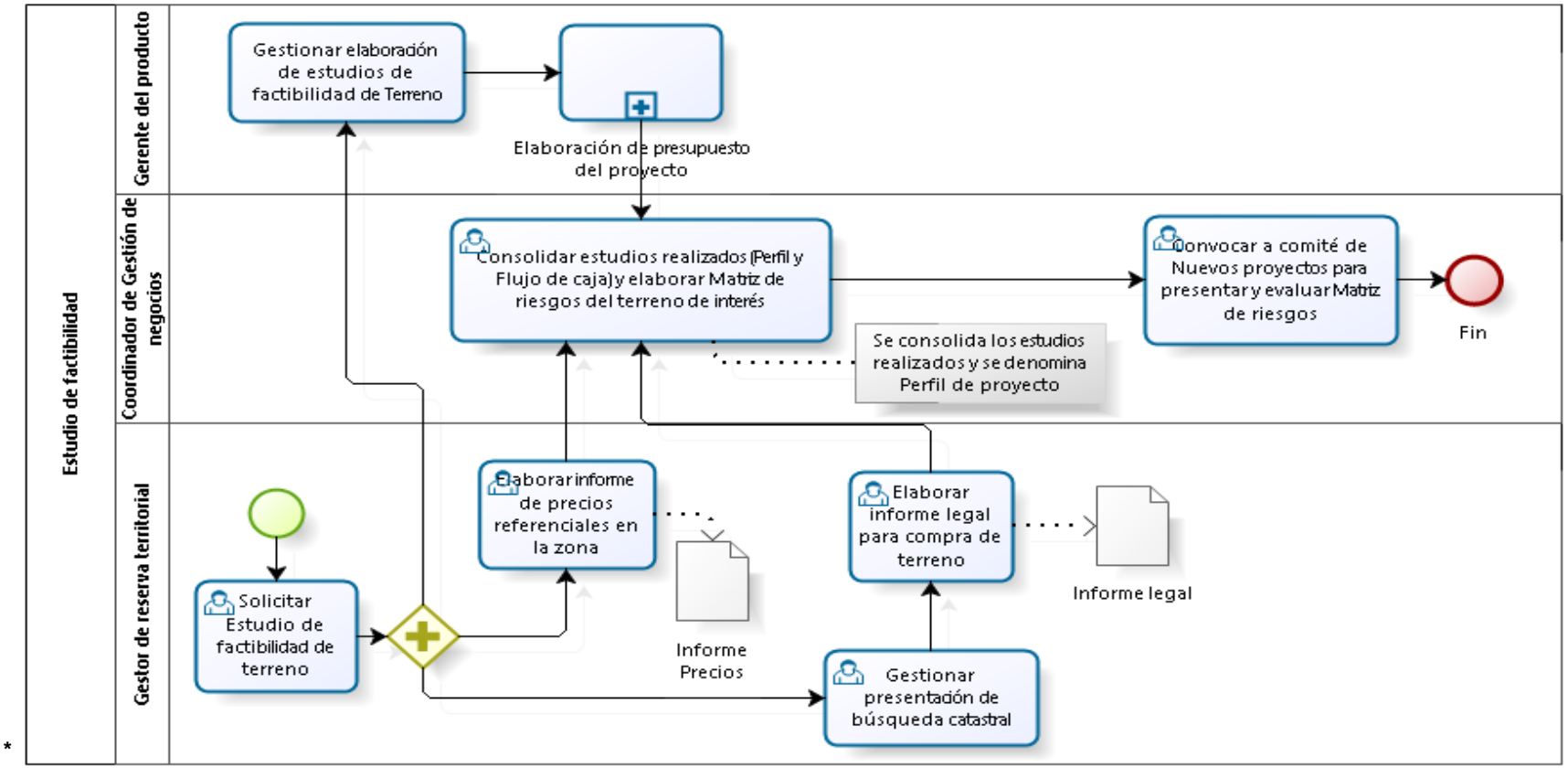
Proceso Búsqueda de terrenos



Proceso Negociación con propietario

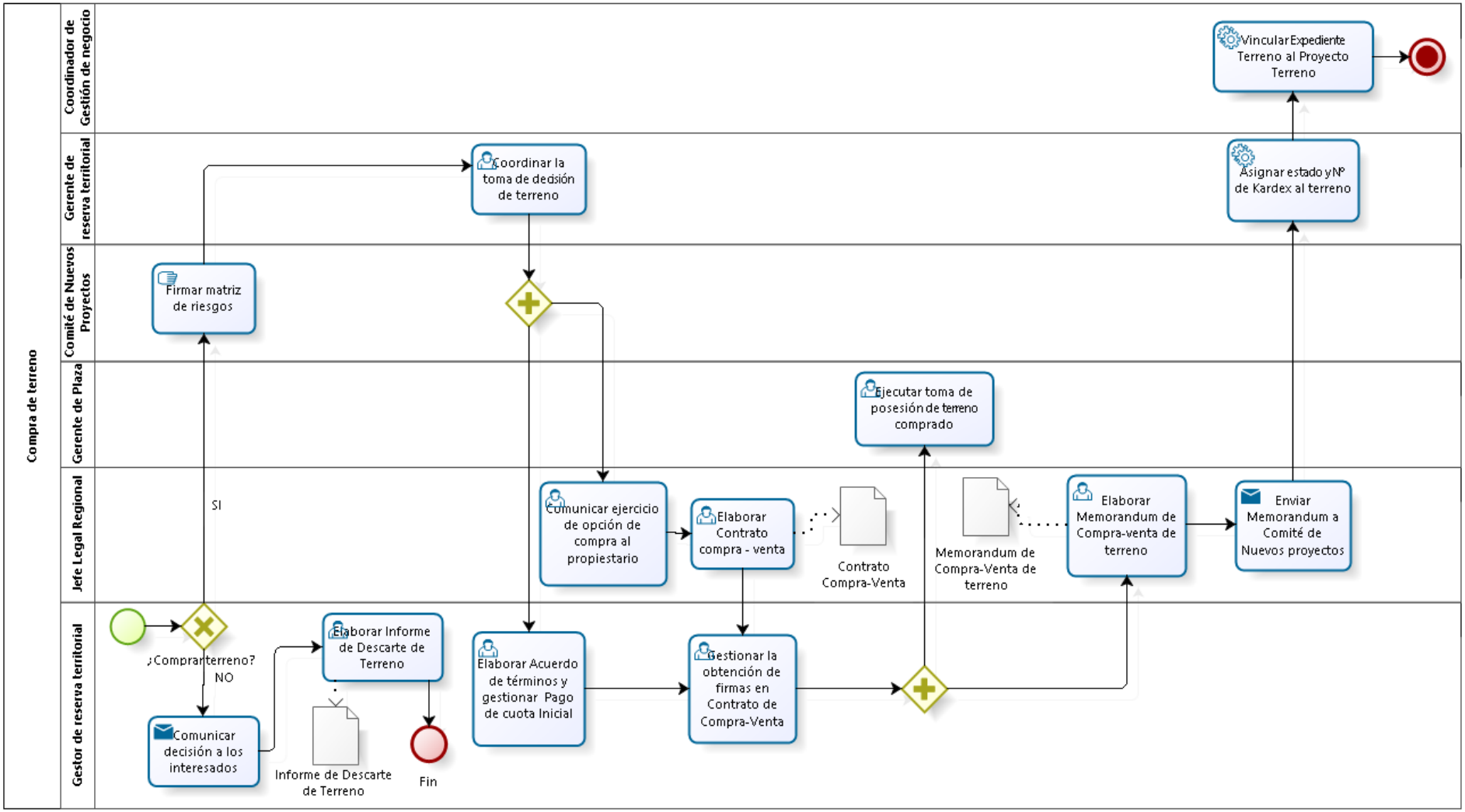


Proceso Estudio de factibilidad

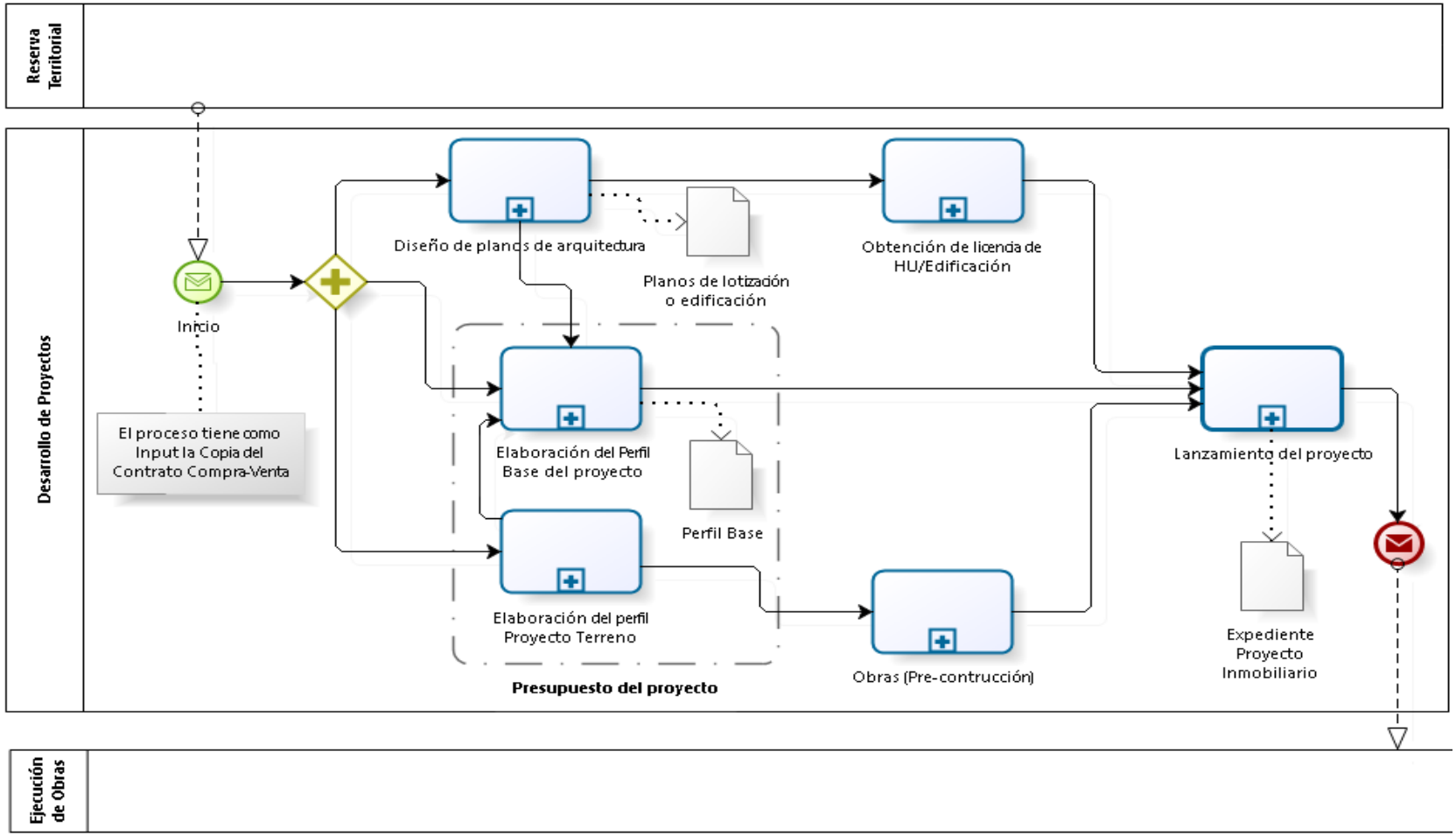


Informe precios, documento con cuadros y gráficos en el cual se indican los precios del terreno de interés y los terrenos colindantes al terreno de interés, el gráfico comprende un mapa de la zona con los precios actuales (Previos a la fecha de compra del terreno) y los cuadros muestran un comparativo de dichos precios (Terreno de interés vs terrenos colindantes)

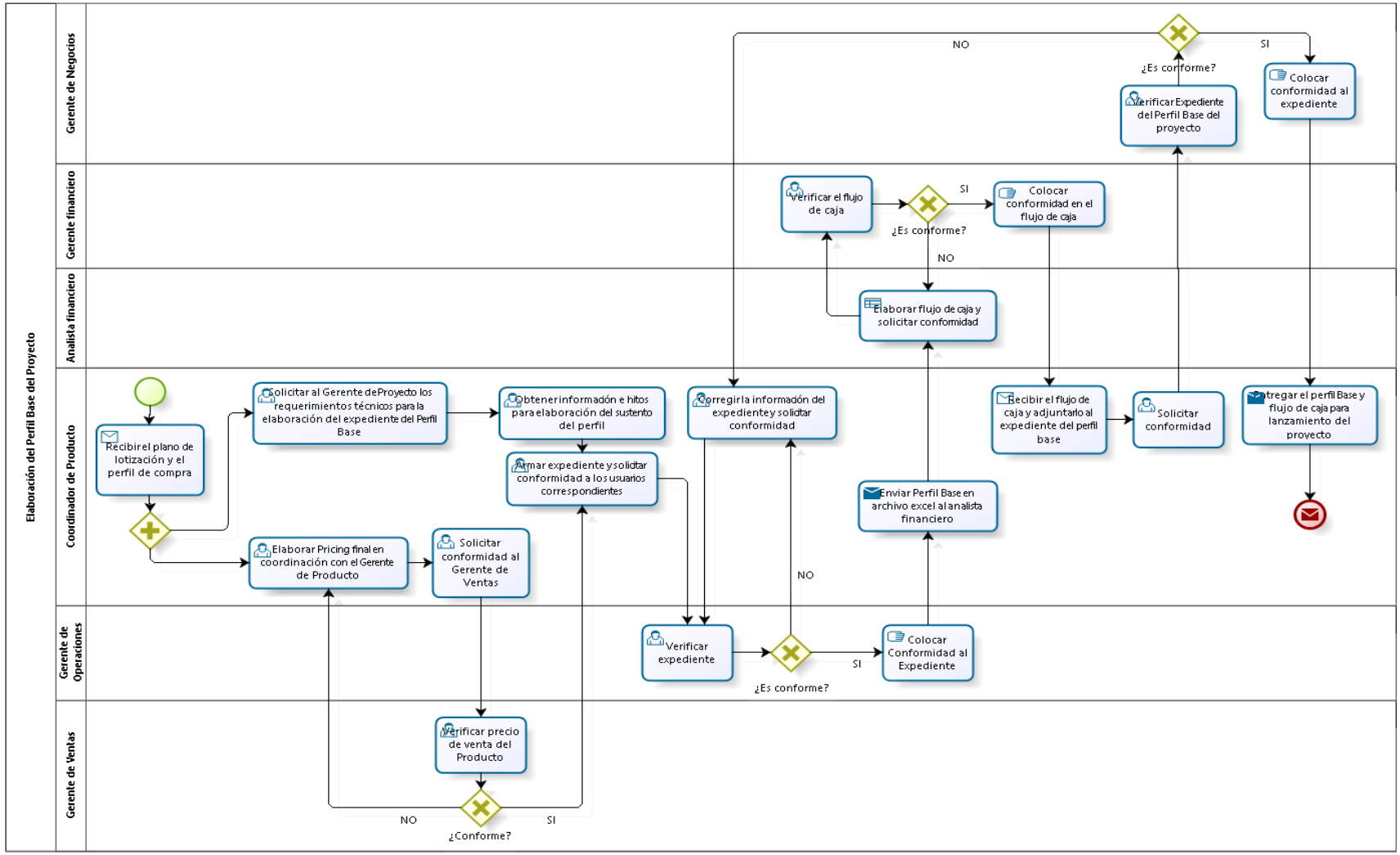
Proceso Compra de Terreno



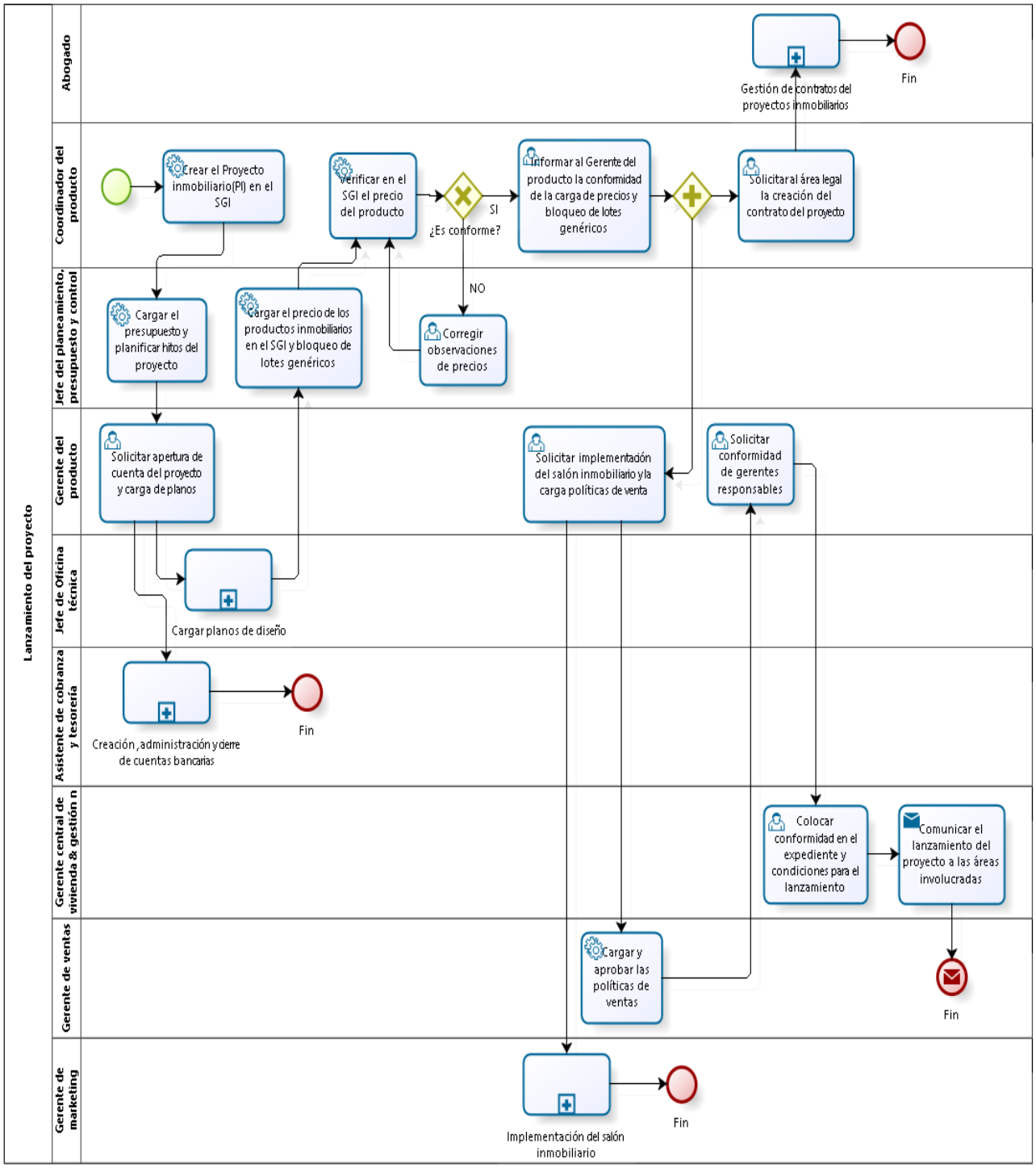
Anexo B.2 Macro-proceso Desarrollo de Proyectos



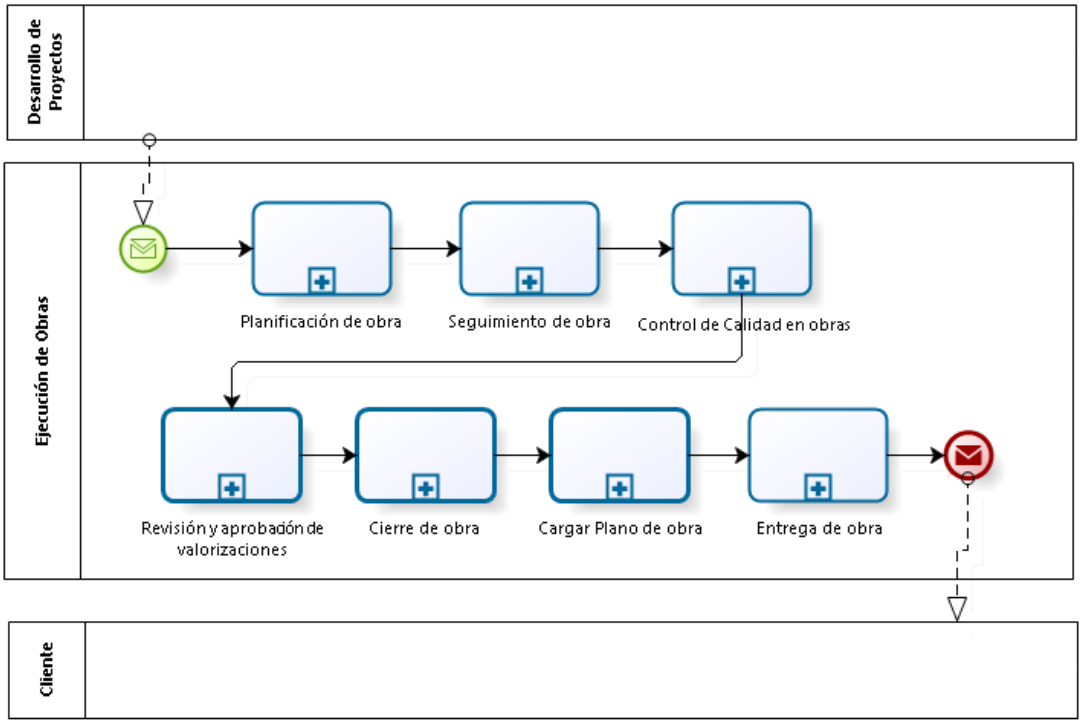
Proceso Elaboración del Perfil Base del Proyecto



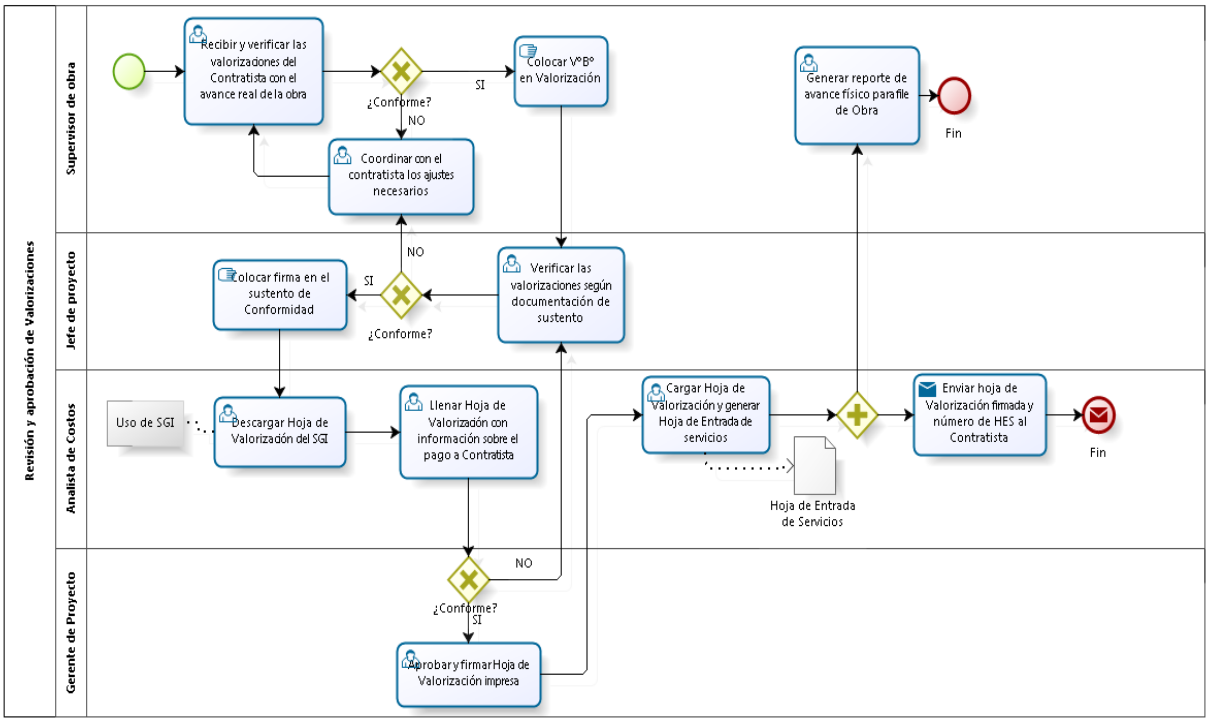
Proceso Lanzamiento de Proyectos



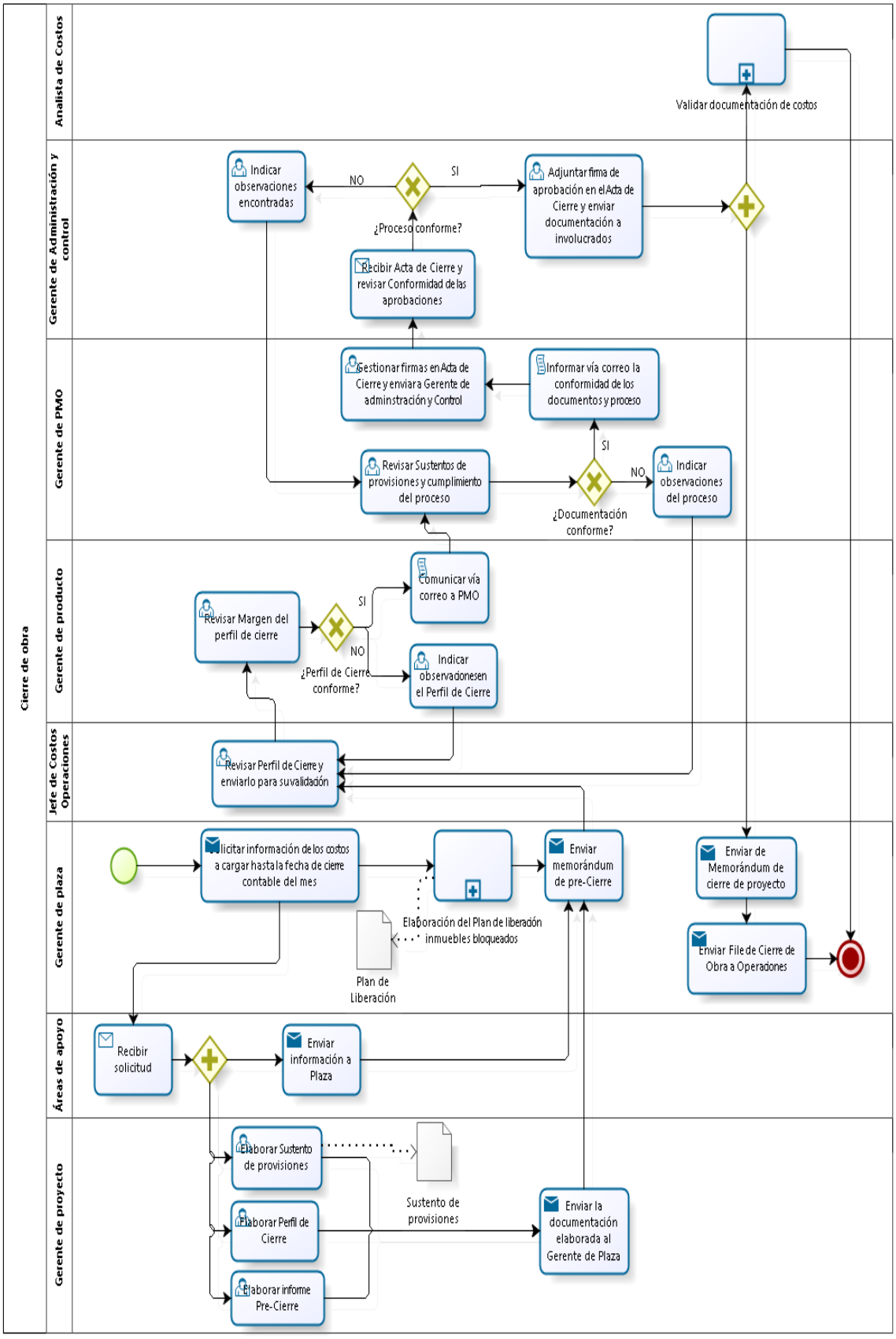
Anexo B.3 Macro-proceso de Ejecución de obras



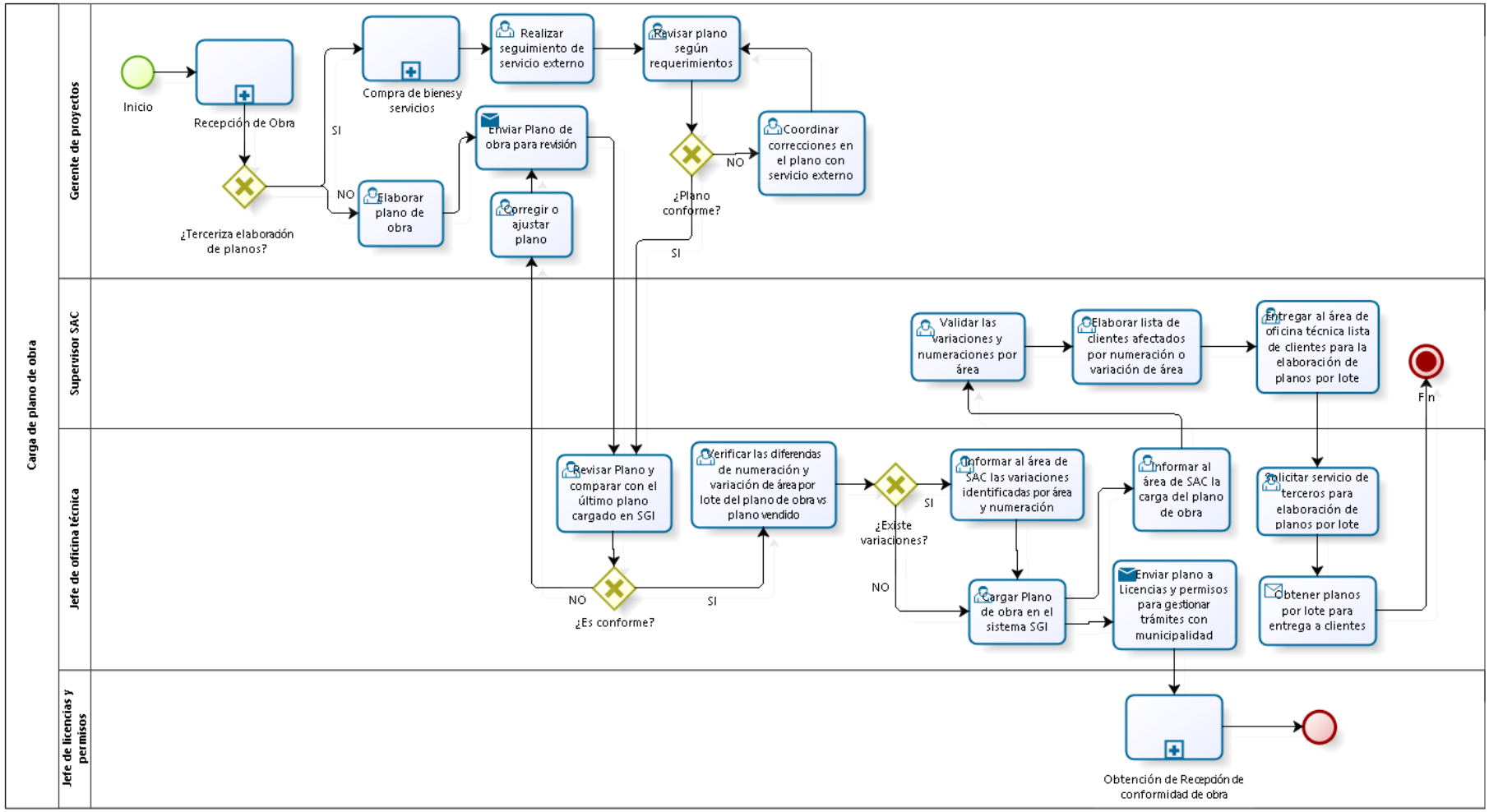
Proceso de Revisión y Aprobación de Valorizaciones



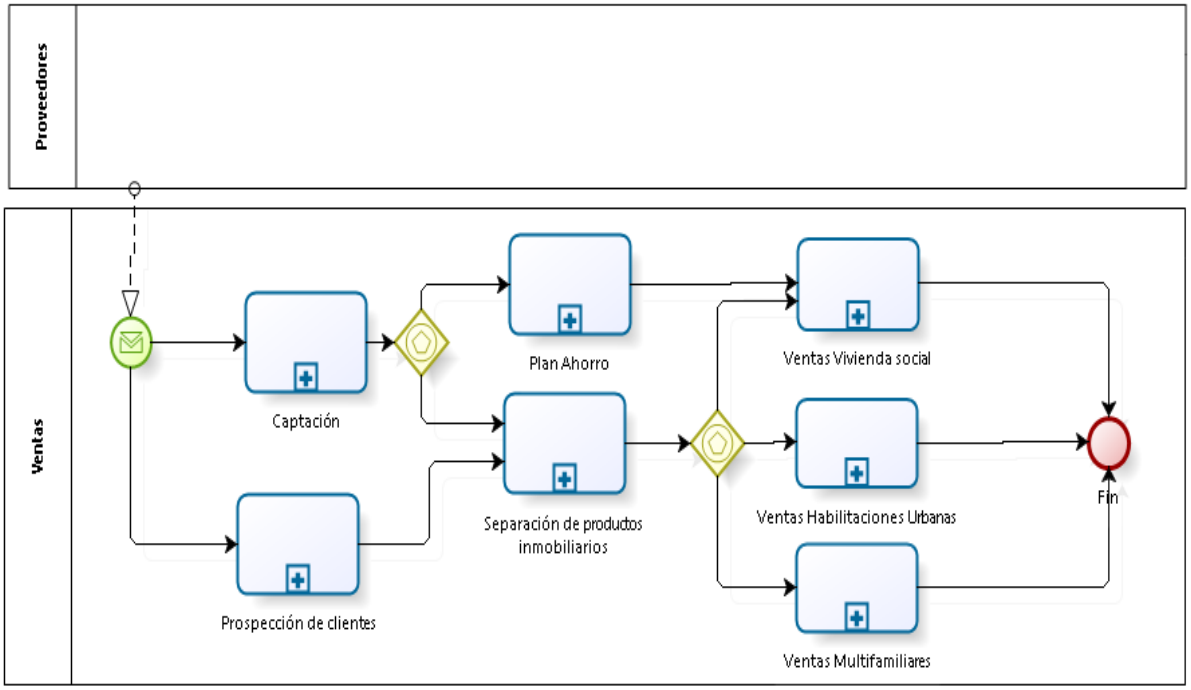
Proceso Cierre de Obra



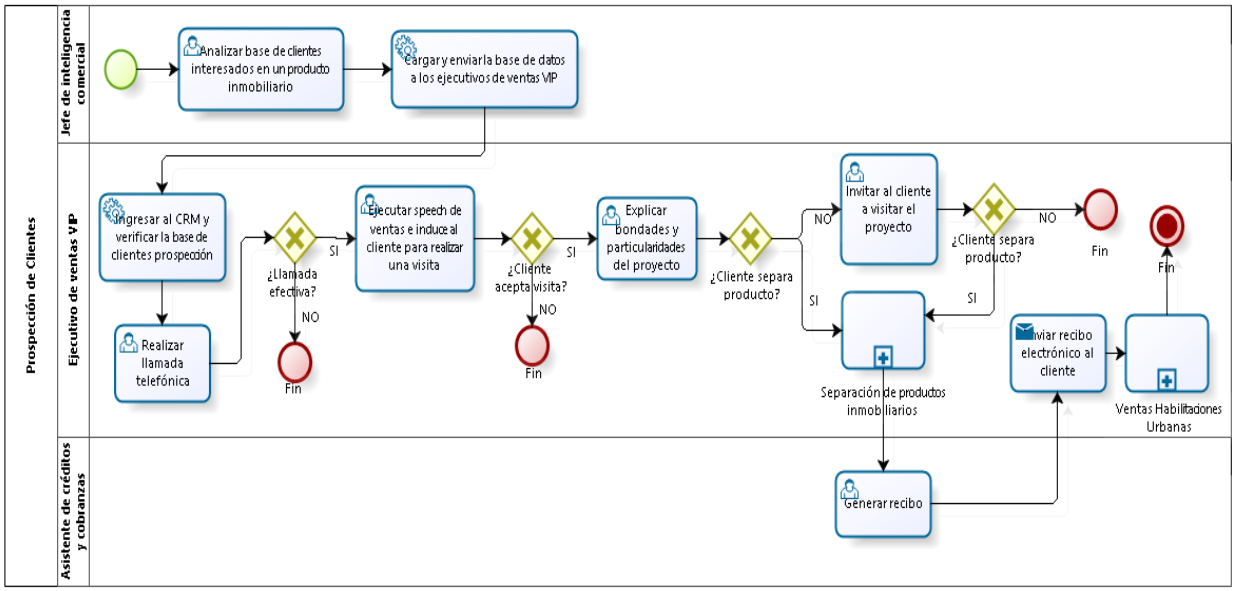
Proceso Carga de plano de Obra



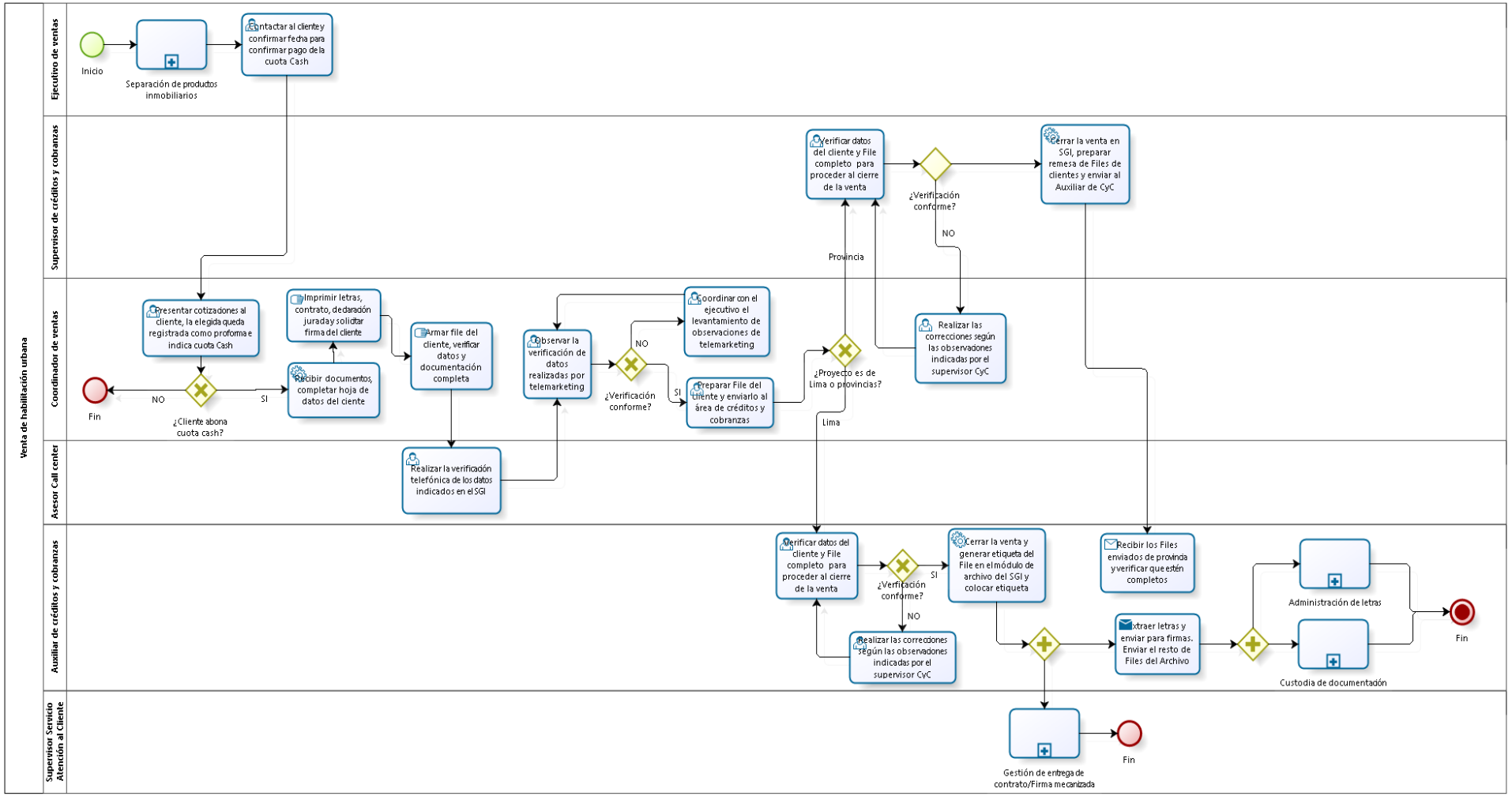
Anexo B.4 Macro-proceso de Ventas



Proceso de Prospección de Clientes

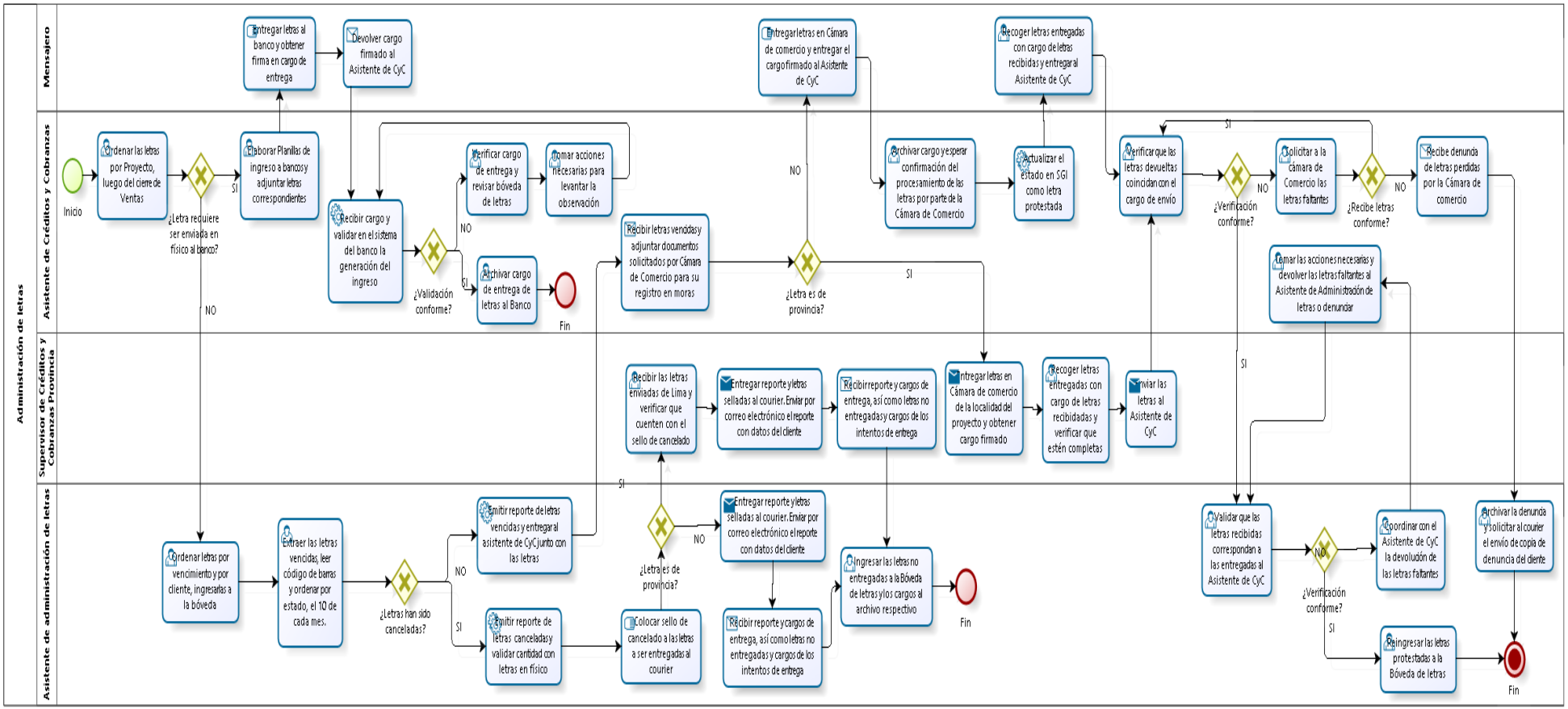


Proceso de Ventas de Habilitación Urbana

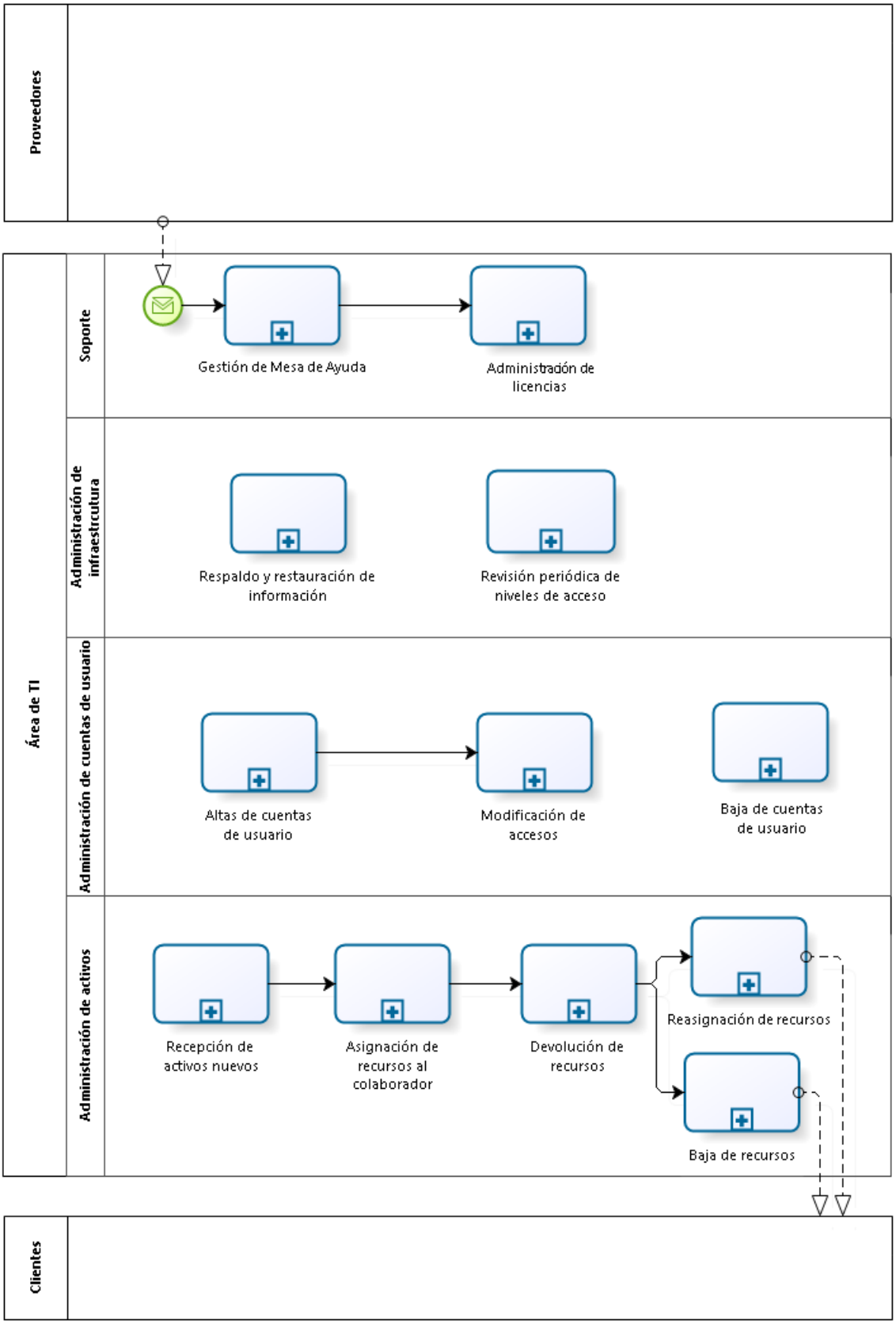


Anexo B.5 Macro-proceso de Cobranzas

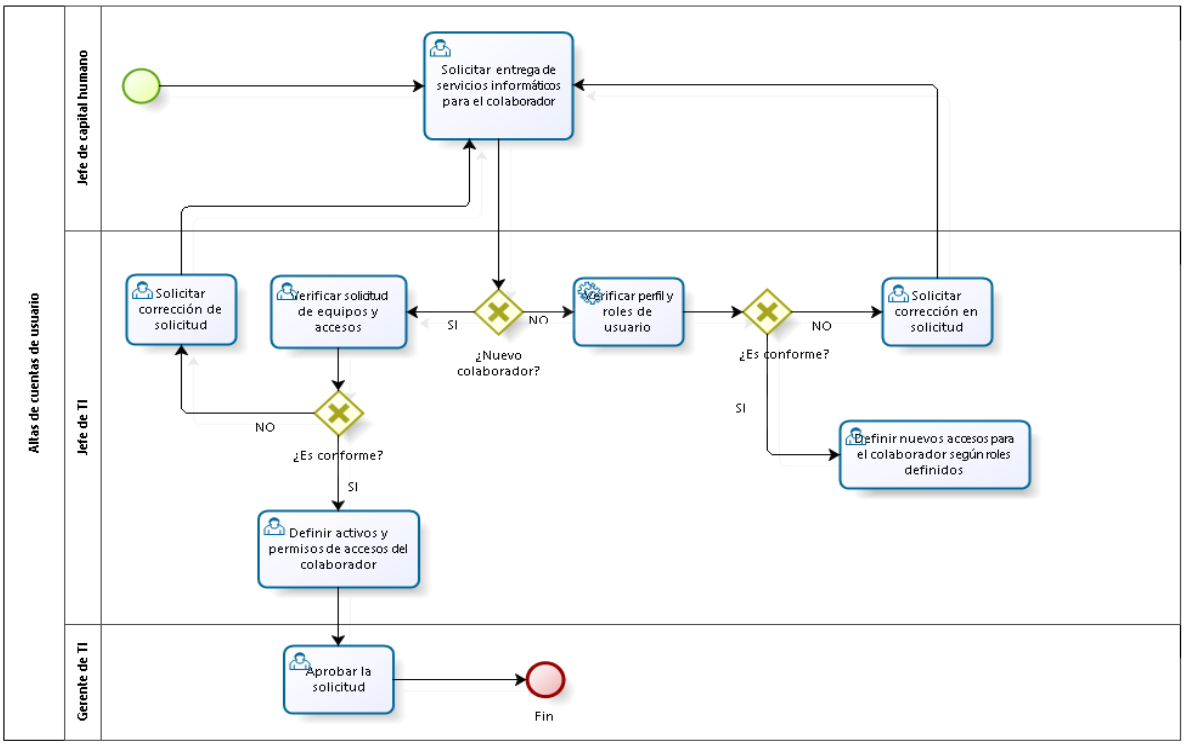
Proceso de Administración de letras



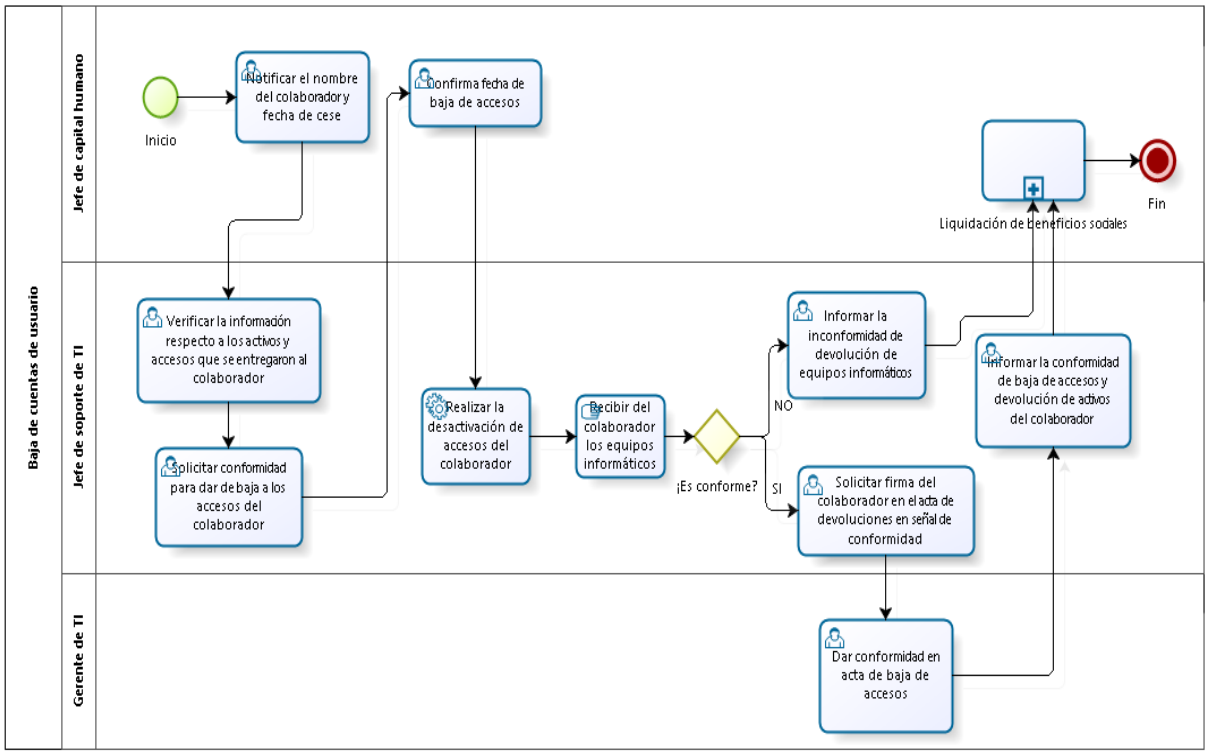
Anexo B.6 Macro-proceso de Tecnología de Información



Proceso de Alta de cuentas de usuario



Proceso de Baja de cuentas de usuario



ANEXO C. Listado de Valorización de Activos

Activo de Información						Proceso		Valorización			
								Criterios			
ID	Tipo	Nombre	Descripción	Propietario	Ubicación	Proceso	Sub-proceso	Disponibilidad	Integridad	Confidencialidad	Valor
01	Datos	Informe de zonas de búsqueda	Documento con una lista detallada de las zonas de terreno de interés	Gerente de Reserva Territorial	Electrónico/Físico	Reserva territorial	Búsqueda de terrenos	4	3	4	4
02	Datos	Informe de zonas de terreno	Documento con una lista detallada de las zonas de terreno con posibilidad de compra, además contiene información de los propietarios.	Gerente de Reserva Territorial	Electrónico/Físico	Reserva territorial	Búsqueda de terrenos	4	3	3	3
03	Datos	Planos de terreno	Plano de levantamiento topográfico del terreno	Gerente de Reserva Territorial	Electrónico/Físico	Reserva territorial	Búsqueda de terrenos	3	4	4	4
04	Datos	Informe Catastral	Memoria descriptiva del plano, incluye los planos.	Gerente de Reserva Territorial	Electrónico/Físico	Reserva territorial	Búsqueda de terrenos	3	3	1	2
05	Datos	Expediente del proyecto	Evaluación de un proyecto para definir la factibilidad del proyecto.	Gestor de Reserva Territorial	Electrónico/Físico	Reserva territorial	Compra de terreno	4	3	3	3
06	Personal	Comité de Nuevos proyectos	Junta interna compuesta por ejecutivos que tiene como objetivo brindar soporte en la toma de decisiones respecto a la viabilidad de los proyectos inmobiliarios.	Comité de Nuevos proyectos	Físico	Reserva territorial	Compra de terreno	4	3	1	3
07	Datos	Informe de Descarte de Terreno	Documento que sustenta la no ejecución de compra de un terreno de interés.	Gestor de Reserva Territorial	Electrónico/Físico	Reserva territorial	Compra de terreno	3	3	2	3
08	Datos	Contrato de compra-venta	Documento con las cláusulas de compra de un terreno.	Jefe legal regional	Físico	Reserva territorial	Compra de terreno	4	4	2	3

Activo de Información						Proceso		Valorización			
								Criterios			
ID	Tipo	Nombre	Descripción	Propietario	Ubicación	Proceso	Sub-proceso	Disponibilidad	Integridad	Confidencialidad	Valor
09	Datos	Memorándum de Contrato de compra-venta	Memoria descriptiva del Contrato de compra	Jefe legal regional	Electrónico	Reserva territorial	Compra de terreno	4	4	2	3
10	Datos	Perfil del proyecto	Consolidado de documentos del proceso de Reserva territorial	Gerente de Gestión de Negocios	Electrónico/Físico	Reserva territorial	Estudio de factibilidad	4	4	4	4
11	Datos	Informe de precios	Documento con cuadros y gráficos en el cual se indican y comparan los precios del terreno de interés y terrenos colindantes.	Gestor de Reserva Territorial	Electrónico/Físico	Reserva territorial	Estudio de factibilidad	4	3	4	4
12	Aplicaciones	Sistema PSAD56	Sistema de información catastral	Jefe legal regional	Electrónico	Reserva territorial	Estudio de factibilidad	4	3	1	3
13	Aplicaciones	SGI	Sistema de Gestión inmobiliaria que soporta todo el proceso de Reserva territorial	Gerente de TI	Electrónico	Reserva territorial	Negociación con propietario	3	3	3	3
14	Datos	Condiciones de negociación	Conjunto de enunciados o condiciones de compra que serán aceptados por el propietario del terreno.	Gerente de Reserva Territorial	Electrónico/Físico	Reserva territorial	Negociación con propietario	3	3	4	3
15	Datos	Contrato de Opción de compra	Documento con las cláusulas de opción compra de un terreno.	Abogado	Físico	Reserva territorial	Negociación con propietario	3	3	1	2
16	Datos	Memorándum de Contrato de Opción de compra	Memoria descriptiva del Contrato de Opción de compra	Abogado	Electrónico/Físico	Reserva territorial	Negociación con propietario	3	4	2	3

Activo de Información						Proceso		Valorización			
								Criterios			
ID	Tipo	Nombre	Descripción	Propietario	Ubicación	Proceso	Sub-proceso	Disponibilidad	Integridad	Confidencialidad	Valor
17	Datos	Expediente del perfil Base	Evaluación de un proyecto para definir la factibilidad (ingresos, costo, margen bruto) del proyecto.	Coordinador de producto	Electrónico/Físico	Desarrollo de proyectos	Elaboración del Perfil Base del proyecto	4	3	3	3
18	Datos	Planos de diseño	Planos de lotización, Planos de trazado, vías y topográfico.	Coordinador de producto	Electrónico/Físico	Desarrollo de proyectos	Elaboración del Perfil Base del proyecto	4	3	3	3
19	Aplicaciones	SGI	Sistema de Gestión inmobiliaria que soporta todo el proceso de Reserva territorial	Gerente de Producto	Electrónico	Desarrollo de proyectos	Lanzamiento del Proyecto	4	3	3	3
20	Aplicaciones	MS Office	Contiene aplicaciones de escritorio, para la elaboración de informes, cuadros, gráficos, entre otros.	Gerente de TI	Electrónico	Todos los procesos	Todos	3	3	3	3
21	Datos	Documento de Valorización	Valorización del contratista con respecto al avance de la obra.	Supervisor de obra	Electrónico/Físico	Ejecución de Obra	Revisión y Aprobación de Valorizaciones	4	3	3	3
22	Datos	Hoja de Entrada de Servicios	Documento que se genera luego de cargar el documento de Valorización al sistema	Analista de costos	Electrónico/Físico	Ejecución de Obra	Revisión y Aprobación de Valorizaciones	4	3	2	3
23	Aplicaciones	SGI	Sistema de Gestión inmobiliaria que soporta todo el proceso de Reserva territorial	Gerente de Producto	Electrónico	Ejecución de Obra	Revisión y Aprobación de Valorizaciones	4	3	2	3
24	Tecnología	Servidor de correo	-	Jefe de TI	Electrónico	Todos los procesos	Todos	4	3	2	3
25	Tecnología	Servidor de aplicaciones	-	Jefe de TI	Electrónico	Todos los procesos	Todos	4	3	2	3

ANEXO D. Mapa de Riesgos

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
RT-01	Reserva territorial	Búsqueda de terrenos	Proveer de un informe de zonas de terrenos aptos para su posible adquisición.	Posible filtración del informe de zonas de búsqueda a otra empresa competidora debido al robo de la información desde la computadora originado por acceso a personal no autorizado.	Clientes, servicios y prácticas institucional	Personal	Una persona que laboraba anteriormente en la empresa no se le ha deshabilitado los accesos.	Ocasional	Crítico	Alto
RT-02				Posible error en la creación del Expediente Terreno debido a fallo en el sistema SGI originado por problemas en el servidor de aplicaciones	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema SGI no funciona o tiene problemas de conexión con el servidor de aplicaciones.	Ocasional	Medio	Alto
RT-03				Posible filtración de la comunicación con el propietario del terreno para una posible compra .	Clientes, servicios y prácticas institucional	Personal	El propietario divulga su comunicación con la empresa para comparar ofertas.	Ocasional	Menor	Moderado
RT-04				Posible extravío de los planos de terreno debido al descuido del personal encargado.	Ejecución, entrega y gestión de procesos	Personal	El personal no tenía adecuadamente archivado los documentos del propietario.	Moderado	Medio	Alto
RT-05				Posible robo de la documentación del predio del propietario debido a la ausencia de personal de seguridad	Clientes, servicios y prácticas institucional	Procesos internos	El personal no se encontraba en su puesto de trabajo	Improbable	Medio	Moderado
RT-06				Posible robo de la documentación del predio del propietario debido a la ausencia de cámaras de seguridad	Clientes, servicios y prácticas institucional	Procesos internos	No hay cámaras de seguridad en el lugar en las que archivan la documentación.	Remoto	Medio	Moderado
RT-07				Posible fraude originado por la recepción de documentación falsa o desactualizada del predio del propietario.	Fraude externo	Personal	El personal encargado de recibir la documentación no fue capaz de validar la información.	Ocasional	Medio	Alto

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
RT-08	Reserva territorial	Negociación con propietario	Elaboración del contrato de opción de compra mediante el establecimiento de condiciones de negociación con el propietario.	Posible modificación de la propuesta con las condiciones de negociación del predio antes de ser entregada al propietario debido a la filtración del mismo originado por descuido del Gestor de Reserva Territorial.	Ejecución, entrega y gestión de procesos	Personal	El personal encargado de enviar la propuesta al propietario perdió los documentos	Remoto	Medio	Moderado
RT-09				Posible fallo en la creación del Proyecto Terreno debido a problemas en el sistema SGI originado por una falla en el servidor de aplicaciones.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema SGI no funciona o tiene problemas de conexión con el servidor de aplicaciones.	Remoto	Medio	Moderado
RT-10				Posible error en la asignación de terrenos a un Proyecto Terreno debido al inadecuado uso de la aplicación originado por la complejidad del sistema SGI.	Ejecución, entrega y gestión de procesos	Tecnología de Información	No se ha realizaso capacitación sobre el sistema SGI al personal encargado.	Ocasional	Crítico	Alto
RT-11				Posible fallo en la asignación de terrenos a un Proyecto Terreno debido a un ataque malicioso originado por un hacker que se infiltró en el sistema SGI.	Interrupción de las operaciones y fallos en los sistemas	Eventos externos	El antivirus está desactualizado.	Remoto	Medio	Moderado
RT-12	Reserva territorial	Estudio de factibilidad	Elaboración del perfil del Proyecto el cuál debe contener el consolidado de los estudios realizados (Presupuesto del proyecto, Matriz de riesgos del terreno de interés, informe	Posible fallo en el envío del correo de solicitud debido a la indisponibilidad de la aplicación de correo electrónico originado por error en el servidor de aplicaciones.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El servidor de aplicaciones se ha visto comprometido por un ataque de denegación de servicio.	Ocasional	Medio	Alto
RT-13				Posible robo del informe de precios referenciales de las zonas de interés debido a la filtración de la información originado por error del personal encargado del envío de la información al coordinador.	Ejecución, entrega y gestión de procesos	Personal	El courier entregó el informe a otra persona.	Remoto	Medio	Moderado

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
RT-14	Reserva territorial	Estudio de factibilidad	Elaboración del perfil del Proyecto el cuál debe contener el consolidado de los estudios realizados (Presupuesto del proyecto, Matriz de riesgos del terreno de interés, informe de precios, informe legal)	Posible robo del informe de precios referenciales de la zona de interés debido a la filtración de la información digital originado por otorgar acceso a personal no autorizado.	Interrupción de las operaciones y fallos en los sistemas	Procesos internos	No hay una lista de perfiles de acceso o está desactualizada.	Ocasional	Medio	Alto
RT-15				Posible error en la elaboración del informe legal para compra de terreno debido a la indisponibilidad de la información del plano originado por falla en el sistema PSAD56	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema PSAD56 no funciona o tiene problemas de conexión con el servidor de aplicaciones.	Improbable	Crítico	Moderado
RT-16				Posible error en la elaboración de la Matriz de riesgos del terreno de interés debido a la indisponibilidad del informe legal originado por retraso en la entrega del plano.	Ejecución, entrega y gestión de procesos	Procesos internos	El jefe legal no dispone con toda la documentación necesaria para realizar el informe.	Ocasional	Crítico	Alto
RT-17				Posible alteración de la información de la Matriz de riesgos del terreno de interés debido a la sustracción de la información originado por el descuido del coordinador de Gestión de Negocios.	Ejecución, entrega y gestión de procesos	Personal	El coordinador de Gestión no archivó adecuadamente algún documento: el flujo de caja, estudios técnicos o el informe de precios.	Ocasional	Medio	Alto
RT-18	Reserva territorial	Compra de terreno	Asegurarse de que los terrenos sean adecuados para los proyectos de la organización.	Posible alteración de la Matriz de riesgos antes de ser aprobada la compra del terreno debido a la filtración de su información originado por otorgar accesos a personal no autorizado.	Fraude interno	Personal	No hay una lista de perfiles de acceso o está desactualizada.	Remoto	Crítico	Alto
RT-19				Posible falsificación de firmas en la Matriz de riesgos debido a una inadecuada verificación de validez de las mismas originado por el descuido del personal encargado.	Fraude interno	Personal	No se validan las firmas de la Matriz de riesgos.	Ocasional	Medio	Alto

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
RT-20	Reserva territorial	Compra de terreno	Asegurarse de que los terrenos sean adecuados para los proyectos de la organización.	Posible retraso en la comunicación de la decisión a los interesados debido a errores en la aplicación de correo originado por falla en la red.	Ejecución, entrega y gestión de procesos	Eventos externos	El servidor de aplicaciones se ha visto comprometido por un ataque de denegación de servicio.	Remoto	Medio	Moderado
RT-21				Posible pérdida de informe de Descarte de Terreno debido a falla del equipo de cómputo en el que se realizó originado por una falla del hardware.	Ejecución, entrega y gestión de procesos	Tecnología de Información	Se ha dañado el disco duro del equipo de cómputo .	Moderado	Medio	Alto
RT-22				Posible error en la elaboración del Acuerdo de términos debido a indisponibilidad de la aplicación originado por falla en el software.	Clientes, servicios y prácticas institucional	Tecnología de Información	No se activaron las licencias de la aplicación.	Remoto	Medio	Moderado
RT-23				Posible inexactitud de la información del contrato de Compra-venta debido a la falta de datos del propietario originado por pérdida de documentación.	Clientes, servicios y prácticas institucional	Personal	Extravío de la documentación del propietario.	Ocasional	Crítico	Alto
RT-24	Reserva territorial	Compra de terreno	Asegurarse de que los terrenos sean adecuados para los proyectos de la organización.	Posible interrupción en la asignación de estado al Expediente Terreno debido a la indisponibilidad del Memorándum de Compra-Venta originado por el retraso del envío.	Interrupción de las operaciones y fallos en los sistemas	Procesos internos	Hay problemas con el envío del memorándum de compra-venta debido a una falla de la aplicación.	Remoto	Medio	Moderado
RT-25				Posible fallo en la asignación de estado y un Nº de Kardex del Expediente Terreno debido a problemas en el sistema SGI originado por una falla en el servidor de aplicaciones.	Ejecución, entrega y gestión de procesos	Tecnología de Información	El servidor de aplicaciones se ha visto comprometido por un ataque de denegación de servicio.	Moderado	Medio	Alto
RT-26				Posible fallo en la vinculación del Expediente Terreno al Proyecto Terreno debido al uso inadecuado del SGI originado por complejidad del sistema.	Ejecución, entrega y gestión de procesos	Personal	No se ha realizaso capacitación sobre el sistema SGI al personal encargado.	Ocasional	Medio	Alto

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
RT-27	Reserva territorial	Compra de terreno	Asegurarse de que los terrenos sean adecuados para los proyectos de la organización.	Posible error al asignar gastos al Expediente Terreno asociados a la compra del terreno debido a una falla en el SGI originado por la intrusión de un malware en el sistema.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema SGI se ha visto comprometido por la infección de un malware.	Remoto	Crítico	Alto
RT-28				Posible error en la comunicación con el proceso de Desarrollo de Proyectos debido a una falla en la aplicación de correo originado por una falla del software.	Clientes, servicios y prácticas institucional	Tecnología de Información	No se tiene acceso a la aplicación de correos debido a una falla del software.	Remoto	Medio	Moderado
DP-01	Desarrollo de Proyectos	Elaboración del Perfil Base del proyecto	Elaborar el expediente del perfil Base y flujo de caja para sustentar la viabilidad del proyecto.	Posible pérdida de información para elaboración del sustento del perfil debido a falla en la laptop usada originado por descuido del Coordinador del producto.	Interrupción de las operaciones y fallos en los sistemas	Personal	El hardware del equipo de cómputo se ha visto comprometido debido a sucesivas caídas de la laptop.	Remoto	Medio	Moderado
DP-02				Posible filtración de los requerimientos técnicos del expediente debido al robo de los planos de diseño originado por otorgar acceso de ingreso a personal no autorizado.	Clientes, servicios y prácticas institucional	Personal	No hay una lista de perfiles de acceso o está desactualizada.	Moderado	Crítico	Extremo
DP-03				Posible pérdida de la información debido al robo del Expediente del perfil Base del proyecto originado por otorgar accesos a personal no autorizado.	Clientes, servicios y prácticas institucional	Personal	Una persona que laboraba anteriormente en la empresa no se le ha deshabilitado los accesos.	Ocasional	Crítico	Alto
DP-04				Posible pérdida de información sobre el Pricing final debido a interrupción de la aplicación utilizada originado por falla en el software.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	No se tiene acceso a la aplicación debido a una falla del software.	Remoto	Medio	Moderado
DP-05				Posible error en la verificación del expediente del perfil Base debido a información faltante originado por la pérdida de algunos documentos.	Interrupción de las operaciones y fallos en los sistemas	Personal	Extravío de la documentación del Pricing y/o planos de diseño.	Improbable	Crítico	Moderado

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
DP-06	Desarrollo de Proyectos	Elaboración del Perfil Base del proyecto	Elaborar el expediente del perfil Base y flujo de caja para sustentar la viabilidad del proyecto.	Posible pérdida de información digital debido a interrupción de la aplicación originado por una falla en el software.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El servidor de aplicaciones se ha visto comprometido por un ataque de denegación de servicio.	Ocasional	Medio	Alto
DP-07				Posible pérdida de información del archivo excel debido a la interrupcion de la aplicación originado por fallas del hardware.	Interrupción de las operaciones y fallos en los sistemas	Personal	El hardware del equipo de cómputo se ha visto comprometido debido a sucesivas caídas de la laptop.	Remoto	Crítico	Alto
DP-08				Posible alteración de la información del archivo excel debido al ataque malicioso originado por un hacker.	Interrupción de las operaciones y fallos en los sistemas	Eventos externos	Infección de troyano en el equipo de cómputo.	Ocasional	Medio	Alto
DP-09				Posible información incompleta del flujo de caja debido a datos faltantes en el archivo excel originado por la falta de información sobre costos de otras áreas.	Ejecución, entrega y gestión de procesos	Procesos internos	No hay control sobre la asignación de costos	Remoto	Medio	Moderado
DP-10				Posible inexactitud del flujo de caja debido a los errores encontrados en el archivo excel originado por las modificaciones realizadas por el coordinador del producto.	Ejecución, entrega y gestión de procesos	Personal	El coordinador del producto envió una versión anterior del archivo.	Ocasional	Crítico	Alto
DP-11				Posible filtración del perfil Base y flujo de caja debido al envío de correo erróneo originado por descuido del personal encargado.	Ejecución, entrega y gestión de procesos	Personal	Las cuentas de correo electrónico no corresponden a los usuarios.	Ocasional	Crítico	Alto

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
DP-12	Desarrollo de Proyectos	Lanzamiento del proyecto	Establecer lineamientos y controles para el inicio y plan de un proyecto inmobiliario que inicia sus operaciones.	Posible fallo en la creación del Proyecto Inmobiliario debido a problemas en el sistema SGI originado por una falla en el servidor de aplicaciones.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema SGI no funciona o tiene problemas de conexión con el servidor de aplicaciones.	Ocasional	Medio	Alto
DP-13				Posible creación del Proyecto Inmobiliario falso debido a la ejecución no autorizada del proceso en el sistema originado por una persona malintencionada.	Ejecución, entrega y gestión de procesos	Personal	No se ha deshabilitado accesos a personas que no laboran en la empresa.	Remoto	Medio	Moderado
DP-14				Posible error en la carga del presupuesto debido a la interrupción del sistema SGI originado por falla en el software.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema SGI no funciona o tiene problemas de conexión con el servidor de aplicaciones.	Remoto	Crítico	Alto
DP-15				Posible error en la carga del presupuesto debido a la interrupción del sistema SGI originado por falla en el servicio de red.	Interrupción de las operaciones y fallos en los sistemas	Eventos externos	Incumplimiento de nivel de servicios por parte del proveedor del servicio de internet.	Remoto	Medio	Moderado
DP-16				Posible falla en la carga de planos de diseño debido al desconocimiento de los usuarios originado por la falta de manuales de uso.	Ejecución, entrega y gestión de procesos	Procesos internos	No se ha realizado los manuales de uso del sistema.	Ocasional	Crítico	Alto
DP-17				Posible error al cargar precios de los productos inmobiliarios debido a la interrupción del sistema originado por una falla en el servicio de internet.	Interrupción de las operaciones y fallos en los sistemas	Eventos externos	Incumplimiento de nivel de servicios por parte del proveedor del servicio de internet.	Improbable	Crítico	Moderado
DP-18				Posible error al cargar precios de los productos inmobiliarios debido a la interrupción del sistema originado por una falla en el servidor de aplicaciones.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema SGI no funciona o tiene problemas de conexión con el servidor de aplicaciones.	Remoto	Crítico	Alto

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
DP-19	Desarrollo de Proyectos	Lanzamiento del proyecto	Establecer lineamientos y controles para el inicio y plan de un proyecto inmobiliario que inicia sus operaciones.	Posible alteración de los precios de los productos inmobiliarios debido a la intrusión de un malware en el sistema originado por falta de configuración del firewall.	Ejecución, entrega y gestión de procesos	Personal	Infección de malware debido a la falta de configuración del firewall.	Remoto	Crítico	Alto
DP-20				Posible alteración de los precios de los productos inmobiliarios debido a la intrusión de un malware en el sistema originado por un hacker.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema SGI no funciona o tiene problemas de desempeño debido al ataque de un hacker.	Remoto	Medio	Moderado
DP-21				Posible alteración de los precios de los productos inmobiliarios debido a la ejecución no autorizada de un proceso originado por personal con acceso al sistema.	Ejecución, entrega y gestión de procesos	Personal	La persona anterior que cubría el puesto, aún no tiene desahibiltado los accesos.	Remoto	Medio	Moderado
DP-22				Posible desbloqueo no autorizados de los lotes genéricos debido a la intrusión a la aplicación originado por una persona con accesos al sistema.	Ejecución, entrega y gestión de procesos	Personal	No hay una lista de perfiles de acceso o está desactualizada.	Ocasional	Crítico	Alto
DP-23				Posible error al cargar las políticas de venta debido a falla en el SGI originado por problemas con el software.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema SGI no funciona o tiene problemas de conexión con el servidor de aplicaciones.	Remoto	Menor	Inferior
DP-24				Posible alteración de las políticas de ventas debido a la intrusión de personal no autorizado originado por otorgar más accesos de los necesarios.	Ejecución, entrega y gestión de procesos	Personal	No hay una lista de perfiles de acceso o está desactualizada.	Ocasional	Crítico	Alto

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Descripción del riesgo				Probabilidad	Impacto	Nivel de riesgo
				Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo			
DP-25	Desarrollo de Proyectos	Lanzamiento del proyecto	Establecer lineamientos y controles para el inicio y plan de un proyecto inmobiliario que inicia sus operaciones.	Posible fallo en la comunicación sobre el lanzamiento debido a la indisponibilidad del servidor de correo originado por una falla en el hardware.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	No se ha realizado el manteniemiento preventivo de los servidores	Improbable	Crítico	Moderado
DP-26				Posible fallo en la comunicación sobre el lanzamiento debido a la indisponibilidad del servidor de correo originado por una falla en el servicio de internet.	Interrupción de las operaciones y fallos en los sistemas	Eventos externos	Incumplimiento de nivel de servicios por parte del proveedor del servicio de internet.	Remoto	Crítico	Alto
DP-27				Posible fallo en la comunicación sobre el lanzamiento debido a la indisponibilidad de las líneas telefónicas originado por una falla en el servicio de red.	Interrupción de las operaciones y fallos en los sistemas	Personal	No se configuraron adecuadamente las líneas telefónicas en la oficina.	Improbable	Crítico	Moderado
EO-01	Ejecución de obras	Revisión y aprobación de valorizaciones	Realizar el seguimiento y control en la revisión y aprobación del avance de la obra presentado por el contratista.	Posible alteración de la información de las valorizaciones del Contratista después de colocar el VºBº debido a los ajustes realizados originados por el supervisor de obra.	Ejecución, entrega y gestión de procesos	Personal	El supervisor de Obra modificó la valorización del contratista.	Improbable	Crítico	Moderado
EO-02				Posible alteración de documentos de sustento debido a la inclusión de información falsa originado por el contratista.	Fraude externo	Personal	El contratista presenta documentos falsos para obtener mayor beneficio en la valorización.	Remoto	Crítico	Alto
EO-03				Posible falsificación de firmas en el sustento de Conformidad debido a una inadecuada verificación de validez de la misma originado por el descuido del personal encargado.	Clientes, servicios y prácticas institucional	Personal	No se verifica la firma del Jefe de proyecto.	Ocasional	Medio	Alto

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
EO-04	Ejecución de obras	Revisión y aprobación de valorizaciones	Realizar el seguimiento y control en la revisión y aprobación del avance de la obra presentado por el contratista.	Posible fallo al descargar Hoja de Valorización debido a la interrupción del SGI originado por fallo del software.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema SGI no funciona o tiene problemas de conexión con el servidor de aplicaciones.	Remoto	Medio	Moderado
EO-05				Posible fallo al descargar Hoja de Valorización debido a problemas en la red originado por fallo del hardware.	Interrupción de las operaciones y fallos en los sistemas	Personal	El equipo de red o algunos switches están fallando	Improbable	Medio	Moderado
EO-06				Posible fallo al descargar Hoja de Valorización debido a la indisponibilidad de la aplicación originado por interrupción del SGI.	Ejecución, entrega y gestión de procesos	Eventos externos	El servidor de aplicaciones se ha visto comprometido por un ataque de denegación de servicio.	Remoto	Medio	Moderado
EO-07				Posible error al cargar la Hoja de Valorización debido a falla en el SGI originado por problemas con el software.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema SGI no funciona o tiene problemas de conexión con el servidor de aplicaciones.	Remoto	Medio	Moderado
EO-08				Posible error al cargar la Hoja de Valorización debido a falla en el SGI originado por problemas con el hardware.	Interrupción de las operaciones y fallos en los sistemas	Personal	El equipo de cómputo se ha dañado a causa del mal uso por parte del personal encargado.	Improbable	Medio	Moderado
EO-09				Posible error al generar Hoja de Entrada de Servicios debido a la interrupción del sistema originado por la intrusión de un malware.	Ejecución, entrega y gestión de procesos	Eventos externos	Filtración de un malware en el equipo de cómputo.	Remoto	Crítico	Alto

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
EO-10	Ejecución de obras	Revisión y aprobación de valorizaciones	Realizar el seguimiento y control en la revisión y aprobación del avance de la obra presentado por el contratista.	Posible error al generar Hoja de Entrada de Servicios debido a la indisponibilidad del sistema originado por falla en el software.	Ejecución, entrega y gestión de procesos	Tecnología de Información	El sistema SGI no funciona o tiene problemas de conexión con el servidor de aplicaciones.	Improbable	Crítico	Moderado
EO-11				Posible error al generar Hoja de Entrada de Servicios debido a la indisponibilidad del sistema originado por falla en el servidor.	Ejecución, entrega y gestión de procesos	Eventos externos	El servidor de aplicaciones se ha visto comprometido por un ataque de denegación de servicio.	Remoto	Crítico	Alto
EO-12				Posible error al generar Hoja de Entrada de Servicios debido a la falla en cargar la Hoja de Valorización originado por problemas con el SGI.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Posible error al cargar la Hoja de Valorización debido a falla en el SGI originado por problemas con el software.	Remoto	Medio	Moderado
EO-13				Posible error al generar el número de la Hoja de Entrada de Servicios debido a una falla al cargar la Hoja de Valorización originado por problemas con el sistema.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema SGI no funciona o tiene problemas de conexión con el servidor de aplicaciones.	Remoto	Crítico	Alto
EO-14				Posible retraso en la generación del reporte de avance físico debido al retraso al cargar la Hoja de Valorización originado por falla en el sistema.	Clientes, servicios y prácticas institucional	Procesos internos	Posible fallo al descargar Hoja de Valorización debido a la indisponibilidad de la aplicación SGI.	Improbable	Medio	Moderado

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
EO-15	Ejecución de obras	Revisión y aprobación de valorizaciones	Realizar el seguimiento y control en la revisión y aprobación del avance de la obra presentado por el contratista.	Posible error en el envío de la Hoja de valorización firmada y número de HES al contratista debido a interrupción de la aplicación de correo originado por falla en el servidor de correos.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El servidor de aplicaciones se ha visto comprometido por un ataque de denegación de servicio.	Remoto	Medio	Moderado
EO-16		Cierre de obra	Definir lineamientos para culminar con las obras del proyecto, pasar de producto en proceso a producto terminado.	Posible error al enviar la solicitud de información de costos a cargar debido a una falla en el sistema de correo originado por fallas en el software.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema de correo tiene problemas de conexión con el servidor.	Remoto	Crítico	Alto
EO-17				Posible error al enviar la solicitud de información de costos a cargar debido a la interrupción en el sistema de correo originado por fallas en el servicio de red.	Interrupción de las operaciones y fallos en los sistemas	Eventos externos	Incumplimiento de nivel de servicios por parte del proveedor del servicio de internet.	Improbable	Crítico	Moderado
EO-18				Posible error en la elaboración del Sustento de provisiones debido a la indisponibilidad de algunas órdenes de compra originado por la pérdida de los mismo.	Ejecución, entrega y gestión de procesos	Procesos internos	Retraso en la elaboración de órdenes de compra.	Improbable	Crítico	Moderado
EO-19				Posible inexactitud en la información del Perfil de Cierre debido a que no se han registrado todos los costos ejecutados del proyecto originado por el descuido del personal encargado.	Ejecución, entrega y gestión de procesos	Personal	El personal encargado de no carga a tiempo los costos del proyecto al sistema.	Ocasional	Medio	Alto
EO-20				Posible inexactitud del Informe Pre-Cierre debido a una mala elaboración de las especificaciones técnicas del terreno construido originado por el personal responsable.	Clientes, servicios y prácticas institucional	Personal	El personal no está suficientemente capacitado para la realización del informe.	Remoto	Medio	Moderado

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
EO-21	Ejecución de obras	Cierre de obra	Definir lineamientos para culminar con las obras del proyecto, pasar de producto en proceso a producto terminado.	Posible pérdida de la documentación elaborada debido al extravío o eliminación del mismo originado por el descuido del personal encargado de enviar.	Ejecución, entrega y gestión de procesos	Personal	Se eliminaron los archivos actualizados de la documentación elaborada.	Improbable	Crítico	Moderado
EO-22				Posible error en el envío del memorándum de pre-cierre debido a la ausencia del plan de liberación originado por un retraso en el proceso.	Ejecución, entrega y gestión de procesos	Procesos internos	Se ha retrasado el procedimiento de elaboración de plan de liberación.	Remoto	Medio	Moderado
EO-23				Posible falla en el envío del memorándum debido a la indisponibilidad del servicio de correo originado por una falla en el servicio de internet.	Interrupción de las operaciones y fallos en los sistemas	Eventos externos	Incumplimiento de nivel de servicios por parte del proveedor del servicio de internet.	Remoto	Crítico	Alto
EO-24				Posible error en la comunicación con vía correo con el Gerente de PMO debido a una falla en la aplicación de correo originado por una falla del servidor de correos.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El servidor de correos se ha visto comprometido por un ataque de denegación de servicio.	Ocasional	Crítico	Alto
EO-25				Posible error en la comunicación con vía correo con el Gerente de PMO debido a una falla en la aplicación de correo originado por una falla del servicio de internet.	Interrupción de las operaciones y fallos en los sistemas	Eventos externos	Incumplimiento de nivel de servicios por parte del proveedor del servicio de internet.	Improbable	Crítico	Moderado
EO-26				Posible inexactitud en la información de sustentos de provisiones debido a la falta de documentación originado por la pérdida del mismo.	Ejecución, entrega y gestión de procesos	Personal	Se eliminaron los archivos actualizados de la documentación elaborada.	Remoto	Crítico	Alto

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
EO-27	Ejecución de obras	Cierre de obra	Definir lineamientos para culminar con las obras del proyecto, pasar de producto en proceso a producto terminado.	Posible error en la información de sustentos de provisiones debido a la falta de documentación originado por el retraso del proceso.	Ejecución, entrega y gestión de procesos	Procesos internos	Se ha retrasado el procedimiento debido a que no se entregaron todos los documentos.	Remoto	Medio	Moderado
EO-28				Posible envío de correo falso indicando conformidad de documentación debido a la intrusión de un malware originado por un hacker.	Fraude externo	Eventos externos	El equipo de cómputo ha sido infectado por un malware.	Remoto	Crítico	Alto
EO-29				Posible retraso al enviar el memorándum del Cierre del proyecto debido a la pérdida de documentación originado por descuido del personal encargado.	Ejecución, entrega y gestión de procesos	Personal	La documentación fue eliminada antes del envío del memorándum.	Improbable	Crítico	Moderado
EO-30		Carga de plano de obra	Contar con la versión final de los planos de los proyectos ejecutados considerando los criterios técnicos respectivos en los tiempos establecidos.	Posible error en la elaboración del plano debido al inadecuado seguimiento del servicio originado por el personal responsable.	Clientes, servicios y prácticas institucional	Personal	Incumplimiento de nivel de servicios por parte del proveedor del servicio de elaboración de planos.	Remoto	Crítico	Alto
EO-31				Posible pérdida del plano debido a la falla de la aplicación originado por fallas del software.	Ejecución, entrega y gestión de procesos	Tecnología de Información	La aplicación no cuenta con las últimas actualizaciones.	Remoto	Crítico	Alto
EO-32				Posible error al enviar el plano para revisión debido a la interrupción de la aplicación de correo originado por falla en el servicio de red.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El servidor de correos tiene problemas de conexión.	Ocasional	Medio	Alto

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
EO-33	Ejecución de obras	Carga de plano de obra	Contar con la versión final de los planos de los proyectos ejecutados considerando los criterios técnicos respectivos en los tiempos establecidos.	Posible retraso en la revisión del último plano cargado debido a la indisponibilidad del sistema SGI para mostrarlo originado por falla en el software.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema SGI no funciona o tiene problemas de conexión con el servidor de aplicaciones.	Remoto	Crítico	Alto
EO-34				Posible retraso en la revisión del último plano cargado debido a que no fue cargado correctamente originado por fallas en el sistema SGI.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Indisponibilidad del sistema SGI.	Remoto	Medio	Moderado
EO-35				Posible error en la revisión y comparación entre planos debido a un mal juicio originado por el personal.	Ejecución, entrega y gestión de procesos	Personal	El personal no está suficientemente capacitado.	Improbable	Crítico	Moderado
EO-36				Posible error al cargar el plano de obra al sistema debido a la indisponibilidad del servicio originado por falla en el servidor.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	No se ha realizado mantenimiento preventivo a los servidores.	Remoto	Crítico	Alto
EO-37				Posible inexactitud del plano de obra cargado en el sistema debido al error en la comparación de planos originado por el personal encargado.	Ejecución, entrega y gestión de procesos	Personal	Posible error en la revisión y comparación entre planos debido a un mal juicio originado por el personal.	Remoto	Crítico	Alto
EO-38				Posible error al elaborar lista de clientes debido a equivocación en las validaciones originado por el supervisor SAC	Ejecución, entrega y gestión de procesos	Personal	El personal no está suficientemente capacitado.	Improbable	Crítico	Moderado

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
EO-39	Ejecución de obras	Carga de plano de obra	Contar con la versión final de los planos de los proyectos ejecutados considerando los criterios técnicos respectivos en los tiempos establecidos.	Posible indisponibilidad de los planos por lote debido al retraso en su elaboración originado por el servicio tercerizado.	Clientes, servicios y prácticas institucional	Eventos externos	Incumplimiento de nivel de servicios por parte del proveedor del servicio de elaboración de planos por lotes.	Remoto	Crítico	Alto
VV-01	Ventas	Prospección de cliente	Venta de productos inmobiliarios a través del canal de ventas de prospección	Posible error al cargar las bases de datos de clientes debido a la indisponibilidad del sistema CRM originado por fallo del software.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Indisponibilidad del sistema CRM debido a problemas de desempeño.	Ocasional	Crítico	Alto
VV-02				Posible filtración de la base de clientes debido a la intrusión de un programa malicioso originado por un hacker.	Fraude externo	Eventos externos	Se detectaron vulnerabilidades en los equipos de cómputo debido a la falta de políticas de seguridad.	Remoto	Catastrófico	Extremo
VV-03				Posible retraso en la consulta de clientes en el CRM debido la indisponibilidad del sistema originado por falla en el equipo de cómputo.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El equipo de cómputo presenta fallas técnicas en el hardware.	Remoto	Medio	Moderado
VV-04				Posible entrega de información falsa sobre los productos a los clientes debido a la falta de actualización de los speech por parte del ejecutivo de ventas.	Clientes, servicios y prácticas institucional	Personal	Se usan speech desactualizados para el ofreciemiento de productos.	Remoto	Crítico	Alto
VV-05				Posible error al enviar el recibo al cliente debido a la falla del servicio de correo originado por falla en el hardware.	Interrupción de las operaciones y fallos en los sistemas	Eventos externos	El servidor de correos se ha visto comprometido por un ataque de denegación de servicio.	Remoto	Crítico	Alto

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
VV-06	Ventas	Prospección de cliente	Venta de productos inmobiliarios a través del canal de ventas de prospección	Posible error al enviar el recibo al cliente debido a la falla del servicio de correo originado por falla en la red.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	La infraestructura de la red no soporta a una gran cantidad de usuarios en conexión.	Remoto	Crítico	Alto
VV-07		Venta de Habilitación urbana	Venta de lotes en las plazas donde la inmobiliaria realiza operaciones.	Posible carga de información falsa en el sistema debido a falsificación de documentos del cliente originado por la inadecuada verificación de datos del cliente.	Ejecución, entrega y gestión de procesos	Procesos internos	Recepción de documentos falsos del cliente, debido a que no se verifican o validan los datos.	Improbable	Crítico	Moderado
VV-08				Posible error al cargar los datos del cliente al SGI debido a la interrupción del sistema originado por falla en el servicio de red de la caseta.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Indisponibilidad del sistema SGI debido a problemas de red.	Ocasional	Crítico	Alto
VV-09				Posible retraso en la consulta de clientes en el SGI debido la indisponibilidad del sistema originado por falla en el servicio de red de la caseta.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema SGI tiene problemas de conexión debido a la baja intensidad de señal de red.	Remoto	Medio	Moderado
VV-10				Posible inexactitud de la información del cliente debido a la pérdida de algunos documentos originado por el descuido del coordinador de ventas.	Ejecución, entrega y gestión de procesos	Personal	Se eliminaron del equipo de cómputo, los archivos actualizados de la documentación elaborada.	Improbable	Crítico	Moderado
VV-11				Posible error al cerrar la venta debido a problemas con el SGI originado por falla con el servidor de aplicaciones.	Ejecución, entrega y gestión de procesos	Tecnología de Información	El sistema SGI no funciona o tiene problemas de conexión con el servidor de aplicaciones.	Remoto	Crítico	Alto
VV-12				Posible filtración de la información de los clientes debido a la intrusión de un malware originado por un hacker.	Fraude externo	Eventos externos	El sistema SGI se ha visto comprometido por un malware debido al ataque en el equipo de cómputo.	Remoto	Catastrófico	Extremo

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
CC-01	Cobranzas	Administración de letras	Control y seguimiento de letras por pagos generados en el proceso de ventas	Posible inconsistencia entre la información registrada en el SGI y en las letras debido al inadecuado registro originado por el personal de venta.	Ejecución, entrega y gestión de procesos	Personal	Inadecuado registro de la información del cliente debido al descuido del personal.	Remoto	Crítico	Alto
CC-02				Posible extravío de las letras debido al descuido del personal encargado originado por la inadecuado proceso de almacenamiento.	Ejecución, entrega y gestión de procesos	Procesos internos	El proceso de almacenamiento de letras no ha sido actualizado.	Remoto	Crítico	Alto
CC-03				Posible extravío de las letras debido al descuido del courier originado por la inadecuado proceso de entrega.	Clientes, servicios y prácticas institucional	Personal	Incumplimiento de nivel de servicio de entrega de las letras por parte del proveedor.	Remoto	Crítico	Alto
CC-04				Posible inconsistencia entre la información registrada en el archivo de ingresos y salidas de letras y letras físicas debido al inadecuado registro originado por el personal de cobranzas.	Ejecución, entrega y gestión de procesos	Personal	Descuido del personal para registrar las letras manualmente.	Improbable	Crítico	Moderado
CC-05				Posible inconsistencias entre la información de letras registrado por el banco y el SGI debido al inadecuado registro originado por el personal encargado.	Ejecución, entrega y gestión de procesos	Personal	Descuido del personal para registrar las letras manualmente.	Improbable	Crítico	Moderado
CC-06				Posible inconsistencias entre la información de letras registrado por el banco y el SGI debido al inadecuado registro originado por el software.	Ejecución, entrega y gestión de procesos	Tecnología de Información	El sistema SGI no funciona o tiene problemas de conexión con el servidor.	Remoto	Crítico	Alto
CC-07				Posible error al actualizar estado de letras debido a fallo en el sistema SGI originado por falla en el servidor.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El servidor de aplicaciones se ha visto comprometido por un ataque de denegación de servicio.	Improbable	Crítico	Moderado

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
TI-01	Tecnología de información	Alta de cuentas de usuario	Establecer lineamientos y controles para la distribución de activos y accesos de los distintos sistemas o aplicativos al colaborador.	Posible error en la asignación de accesos a usuarios debido a la ausencia de una matriz de perfiles en la organización originado por falta de documentación.	Ejecución, entrega y gestión de procesos	Procesos internos	El proceso documentado no está debidamente actualizado.	Moderado	Crítico	Extremo
TI-02				Posible fraude interno debido a la asignación de activos y/o aplicativos a usuarios no autorizados originado por error del personal encargado.	Fraude interno	Personal	El personal de TI no actualiza la lista de perfiles de usuario o está mal hecho.	Remoto	Crítico	Alto
TI-03				Posible duplicidad de perfiles y que estos tengan diferentes accesos debido a la inadecuada revisión de la lista de perfiles originado por el encargado.	Ejecución, entrega y gestión de procesos	Personal	El personal de TI no actualiza la lista de perfiles de usuario o está mal hecho.	Improbable	Crítico	Moderado
TI-04				Posible duplicidad de accesos en diferentes perfiles no autorizados debido al inadecuado asignación de accesos originado por error del personal de soporte.	Ejecución, entrega y gestión de procesos	Personal	El personal de TI no actualiza la lista de perfiles de usuario o está mal hecho.	Improbable	Crítico	Moderado
TI-05		Baja de cuentas de usuario	Normar los controles de baja de accesos de usuario para el aseguramiento del proceso de recuperación de credenciales.	Posible error en la desactivación de accesos al colaborador equivocado debido al error del personal originada por una lista de perfiles de acceso desactualizada.	Ejecución, entrega y gestión de procesos	Personal	El personal de TI no actualiza la lista de perfiles de usuario o está mal hecho.	Improbable	Crítico	Moderado
TI-06				Posible fraude externo debido al acceso no autorizado de un excolaborador que tuvo dos perfiles activos, al cual sólo se desactivaron los accesos de un solo perfil.	Fraude externo	Personal	Los perfiles de acceso no son desactivados en el momento oportuno.	Remoto	Crítico	Alto

IDENTIFICACIÓN DE RIESGOS								EVALUACIÓN DE RIESGOS		
				Descripción del riesgo						
Cód. Riesgo	Proceso	Subproceso	Objetivo del proceso	Formulación del riesgo	Tipo riesgo	Tipo evento	Descripción de la causa del riesgo	Probabilidad	Impacto	Nivel de riesgo
TI-07	Tecnología de información	Administración de Infraestructura de TI	Garantizar la funcionalidad y estabilidad de la infraestructura de redes y centros de procesamiento.	Posible interrupción o compromiso del servidor de aplicaciones debido a un ataque de denegación de servicio originado por la infección de un troyano.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Un equipo fue infectado por un troyano, a partir de esto se realizó un ataque de denegación de servicio.	Remoto	Crítico	Alto
TI-08				Posible interrrupción en el funcionamiento de sistemas de información debido a la destrucción o daño de las instalaciones de procesamiento de datos originado por un terremoto en la zona.	Interrupción de las operaciones y fallos en los sistemas	Eventos externos	Desastres naturales o terremotos.	Remoto	Catastrófico	Extremo
TI-09				Posible alteración de los datos almacenados de forma magnética debido a fallos en el funcionamiento de los equipos de cómputo originado por fallos en el suministro eléctrico.	Interrupción de las operaciones y fallos en los sistemas	Eventos externos	Fallas en el suministro eléctrico del edificio.	Improbable	Catastrófico	Alto
TI-10				Posible filtración de información de colaboradores de la organización debido al ataque con un malware originado por un hacker.	Fraude externo	Eventos externos	Ataque de un malware en algún equipo de cómputo.	Remoto	Crítico	Alto

ANEXO E. Plan de Tratamiento de los Riesgos

IDENTIFICACIÓN DE RIESGOS			EVALUACIÓN DE RIESGOS	TRATAMIENTO DE RIESGOS						
Cód. Riesgo	Proceso	Formulación del riesgo	Nivel de riesgo	Estrategia de respuesta	Plan de contingencia	Tipo de control	Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Responsable del proceso	Responsable del control
RT-01	Reserva territorial	Posible filtración del informe de zonas de búsqueda a otra empresa competidora debido al robo de la información desde la computadora originado por acceso a personal no autorizado.	Alto	Evitar	Deshabilitar o eliminar usuarios que han dejado la organización.	Preventivo	9. CONTROL DE ACCESOS.	9.2.1	Gestor de Negocios	Gerente de Negocios
RT-02		Posible error en la creación del Expediente Terreno debido a fallo en el sistema SGI originado por problemas en el servidor de aplicaciones	Alto	Reducir	Realizar regularmente el mantenimiento de los servidores.	Preventivo	11. SEGURIDAD FÍSICA Y DEL ENTORNO.	11.2.4	Gestor de Reserva Territorial	Gerente de Reserva Territorial
RT-04		Posible extravío de los planos de terreno debido al descuido del personal encargado.	Alto	Reducir	Archivar y clasificar la documentación. Colocar cámaras de seguridad en las oficinas en las que se recibe.	Detectivo	8. GESTIÓN DE ACTIVOS. 11. SEGURIDAD FÍSICA Y DEL ENTORNO.	8.2.1 11.1.3	Gestor de Reserva Territorial	Gerente de Reserva Territorial
RT-07		Posible fraude originado por la recepción de documentación falsa o desactualizada del predio del propietario.	Alto	Reducir	Establecer políticas y procedimientos sobre la verificación y validación de documentos.	Preventivo	8. GESTIÓN DE ACTIVOS.	8.2.3	Gestor de Reserva Territorial	Gerente de Reserva Territorial
RT-10		Posible error en la asignación de terrenos a un Proyecto Terreno debido al inadecuado uso de la aplicación originado por la complejidad del sistema SGI.	Alto	Evitar	Realizar capacitaciones al personal que usará el sistema.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES.	12.1.1	Coordinador de Gestión de negocios	Gerente de Negocios
RT-12		Posible fallo en el envío del correo de solicitud debido a la indisponibilidad de la aplicación de correo electrónico originado por error en el servidor de aplicaciones.	Alto	Reducir	Monitoreo exhaustivo de los servidores y aplicaciones. Controles contra malware.	Detectivo	12. SEGURIDAD EN LAS OPERACIONES.	12.2.1	Jefe de soporte de TI	Gerente de TI
RT-14		Posible robo del informe de precios referenciales de la zona de interés debido a la filtración de la información digital originado por otorgar acceso a personal no autorizado.	Alto	Reducir	Establecer políticas sobre la matriz de perfiles de usuario y gestión de accesos.	Correctivo	9. CONTROL DE ACCESOS.	9.1.1	Gestor de Reserva Territorial	Gerente de Reserva Territorial

IDENTIFICACIÓN DE RIESGOS			EVALUACIÓN DE RIESGOS	TRATAMIENTO DE RIESGOS						
Cód. Riesgo	Proceso	Formulación del riesgo	Nivel de riesgo	Estrategia de respuesta	Plan de contingencia	Tipo de control	Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Responsable del proceso	Responsable del control
RT-16	Reserva territorial	Posible error en la elaboración de la Matriz de riesgos del terreno de interés debido a la indisponibilidad del informe legal originado por retraso en la entrega del plano.	Alto	Reducir	Establecer políticas y documentarlas en los procesos correspondientes.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES.	12.1.1	Coordinador de Gestión de Negocios	Gerente de Negocios
RT-17		Posible alteración de la información de la Matriz de riesgos del terreno de interés debido a la sustracción de la información originado por el descuido del coordinador de Gestión de Negocios.	Alto	Evitar	Establecer políticas de escritorios y pantallas limpias en la organización	Preventivo	11. SEGURIDAD FÍSICA Y DEL ENTORNO.	11.2.9	Coordinador de Gestión de Negocios	Gerente de Negocios
RT-18		Posible alteración de la Matriz de riesgos antes de ser aprobada la compra del terreno debido a la filtración de su información originado por otorgar accesos a personal no autorizado.	Alto	Reducir	Establecer políticas sobre la matriz de perfiles de usuario y gestión de accesos.	Correctivo	9. CONTROL DE ACCESOS.	9.2.3 9.2.6	Coordinador de Gestión de negocios	Gerente de Negocios
RT-19		Posible falsificación de firmas en la Matriz de riesgos debido a una inadecuada verificación de validez de las mismas originado por el descuido del personal encargado.	Alto	Reducir	Validar y verificar la legitimidad de las firmas de la Matriz.	Preventivo	7. SEGURIDAD EN LOS RECURSOS HUMANOS.	7.2.2	Comité de Nuevos Proyectos	Gerente de Negocios
RT-21		Posible pérdida de informe de Descarte de Terreno debido a falla del equipo de cómputo en el que se realizó originado por una falla del hardware.	Alto	Reducir	Realizar backups de la información.	Preventivo	11. SEGURIDAD FÍSICA Y DEL ENTORNO.	11.2.4	Gestor de Reserva Territorial	Gerente de Reserva Territorial
RT-23		Posible inexactitud de la información del contrato de Compra-venta debido a la falta de datos del propietario originado por pérdida de documentación.	Alto	Reducir	Establecer políticas de respaldo de información, realizar backups.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES. 18. CUMPLIMIENTO	12.3.1 18.1.3	Jefe legal regional	Gerente de Reserva Territorial
RT-25		Posible fallo en la asignación de estado y un Nº de Kardex del Expediente Terreno debido a problemas en el sistema SGI originado por una falla en el servidor de aplicaciones.	Alto	Reducir	Monitorear y hacer seguimiento a las operaciones del servidor.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES. 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	12.6.1 16.1.5	Gerente de Reserva Territorial	Jefe de TI

IDENTIFICACIÓN DE RIESGOS			EVALUACIÓN DE RIESGOS	TRATAMIENTO DE RIESGOS						
Cód. Riesgo	Proceso	Formulación del riesgo	Nivel de riesgo	Estrategia de respuesta	Plan de contingencia	Tipo de control	Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Responsable del proceso	Responsable del control
RT-26	Reserva territorial	Posible fallo en la vinculación del Expediente Terreno al Proyecto Terreno debido al uso inadecuado del SGI originado por complejidad del sistema.	Alto	Evitar	Realizar capacitaciones al personal que usará el sistema.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES.	12.1.1	Coordinador de Gestión de negocios	Jefe de TI
RT-27		Posible error al asignar gastos al Expediente Terreno asociados a la compra del terreno debido a una falla en el SGI originado por la intrusión de un malware en el sistema.	Alto	Reducir	El sistema debe contar con especificaciones técnicas de seguridad para evitar la intrusión de malware.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES. 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS.	12.2.1 14.1.1	Coordinador de Gestión de negocios	Jefe de TI
DP-02	Desarrollo de Proyecto	Posible filtración de los requerimientos técnicos del expediente debido al robo de los planos de diseño originado por otorgar acceso de ingreso a personal no autorizado.	Extremo	Reducir	Se debe controlar y restringir el derecho a los accesos privilegiados.	Correctivo	9. CONTROL DE ACCESOS.	9.2.3 9.4.1	Coordinador del producto	Gerente del producto
DP-03		Posible pérdida de la información debido al robo del Expediente del perfil Base del proyecto originado por otorgar accesos a personal no autorizado.	Alto	Reducir	Actualizar lista de perfiles de acceso de la empresa.	Correctivo	9. CONTROL DE ACCESOS.	9.2.5 9.4.1	Coordinador del producto	Jefe de TI
DP-06		Posible pérdida de información digital debido a interrupción de la aplicación originado por una falla en el software.	Alto	Reducir	Monitorear y hacer seguimiento a las operaciones del servidor.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES. 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	12.6.1 16.1.5	Coordinador del producto	Jefe de TI
DP-07		Posible pérdida de información del archivo excel debido a la interrupcion de la aplicación originado por fallas del hardware.	Alto	Reducir	Realizar backups de la información.	Preventivo	11. SEGURIDAD FÍSICA Y DEL ENTORNO.	11.2.4	Coordinador del producto	Jefe de TI
DP-08		Posible alteración de la información del archivo excel debido al ataque malicioso originado por un hacker.	Alto	Reducir	Restringir accesos a páginas de internet con dudoso contenido.	Detectivo	12. SEGURIDAD EN LAS OPERACIONES.	12.2.1	Coordinador del producto	Jefe de TI
DP-10		Posible inexactitud del flujo de caja debido a los errores encontrados en el archivo excel originado por las modificaciones realizadas por el coordinador del producto.	Alto	Reducir	Llevar un control de versiones de documentos.	Preventivo	9. CONTROL DE ACCESOS 12. SEGURIDAD EN LAS OPERACIONES.	9.4.2 12.3.1	Coordinador del producto	Gerente de producto

IDENTIFICACIÓN DE RIESGOS			EVALUACIÓN DE RIESGOS	TRATAMIENTO DE RIESGOS						
Cód. Riesgo	Proceso	Formulación del riesgo	Nivel de riesgo	Estrategia de respuesta	Plan de contingencia	Tipo de control	Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Responsable del proceso	Responsable del control
DP-11	Desarrollo de Proyecto	Posible filtración del perfil Base y flujo de caja debido al envío de correo erróneo originado por descuido del personal encargado.	Alto	Evitar	Establecer políticas de seguridad con respecto al uso de correo electrónico.	Preventivo	7. SEGURIDAD EN LOS RECURSOS HUMANOS 13. SEGURIDAD EN LAS COMUNICACIONES.	7.2.2 13.2.1	Coordinador del producto	Gerente de producto
DP-12		Posible fallo en la creación del Proyecto Inmobiliario debido a problemas en el sistema SGI originado por una falla en el servidor de aplicaciones.	Alto	Reducir	Realizar regularmente el mantenimiento de los servidores.	Preventivo	11. SEGURIDAD FÍSICA Y DEL ENTORNO. 12. SEGURIDAD EN LAS OPERACIONES.	11.2.4 12.1.3	Coordinador del producto	Jefe de TI
DP-14		Posible error en la carga del presupuesto debido a la interrupción del sistema SGI originado por falla en el software.	Alto	Reducir	Realizar regularmente el mantenimiento del sistema SGI.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES.	12.1.3	Jefe de planeamiento, presupuesto y control	Jefe de TI
DP-16		Posible falla en la carga de planos de diseño debido al desconocimiento de los usuarios originado por la falta de manuales de uso.	Alto	Evitar	Actualización de los procesos y manuales respectivos.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES.	12.1.1	Jefe de oficina técnica	Gerente de producto
DP-18		Posible error al cargar precios de los productos inmobiliarios debido a la interrupción del sistema originado por una falla en el servidor de aplicaciones.	Alto	Reducir	Realizar regularmente el mantenimiento de los servidores.	Preventivo	11. SEGURIDAD FÍSICA Y DEL ENTORNO. 12. SEGURIDAD EN LAS OPERACIONES.	11.2.4 12.1.3	Jefe de planeamiento, presupuesto y control	Jefe de TI
DP-19		Posible alteración de los precios de los productos inmobiliarios debido a la intrusión de un malware en el sistema originado por falta de configuración del firewall.	Alto	Reducir	Monitoreo en la infraestructura de red.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES. 13. SEGURIDAD EN LAS COMUNICACIONES.	12.2.1 13.1.1	Jefe de planeamiento, presupuesto y control	Jefe de TI
DP-22		Posible desbloqueo no autorizados de los lotes genéricos debido a la intrusión a la aplicación originado por una persona con accesos al sistema.	Alto	Evitar	Supervisar la actividad cada vez que se realice.	Correctivo	9. CONTROL DE ACCESOS.	9.2.6 9.4.1 9.4.4	Jefe de planeamiento, presupuesto y control	Jefe de TI
DP-24		Posible alteración de las políticas de ventas debido a la intrusión de personal no autorizado originado por otorgar más accesos de los necesarios.	Alto	Evitar	Actualizar lista de perfiles de acceso de la empresa.	Correctivo	9. CONTROL DE ACCESOS.	9.2.5 9.4.1	Gerente de Ventas	Jefe de TI

IDENTIFICACIÓN DE RIESGOS			EVALUACIÓN DE RIESGOS	TRATAMIENTO DE RIESGOS						
Cód. Riesgo	Proceso	Formulación del riesgo	Nivel de riesgo	Estrategia de respuesta	Plan de contingencia	Tipo de control	Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Responsable del proceso	Responsable del control
DP-26	Desarrollo de Proyecto	Posible fallo en la comunicación sobre el lanzamiento debido a la indisponibilidad del servidor de correo originado por una falla en el servicio de internet.	Alto	Evitar	Establecer condiciones en caso de incumplimiento del servicio	Preventivo	15. RELACIONES CON PROVEEDORES.	15.2.1	Gerente Central de Vivienda	Gerente Central de Vivienda
EO-02	Ejecución de Obra	Posible alteración de documentos de sustento debido a la inclusión de información falsa originado por el contratista.	Alto	Reducir	Establecer políticas sobre la verificación y validación de documentos.	Preventivo	5. POLÍTICAS DE SEGURIDAD. 8. GESTIÓN DE ACTIVOS	5.1.1 8.2.3	Jefe de proyecto	Gerente de proyecto
EO-03		Posible falsificación de firmas en el sustento de Conformidad debido a una inadecuada verificación de validez de la misma originado por el descuido del personal encargado.	Alto	Reducir	Validar y verificar la legitimidad de las firmas de la Matriz.	Preventivo	6. ORGANIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN 7. SEGURIDAD EN LOS RECURSOS HUMANOS.	6.1.1 7.2.2	Analista de costos	Jefe de costos
EO-09		Posible error al generar Hoja de Entrada de Servicios debido a la interrupción del sistema originado por la intrusión de un malware.	Alto	Reducir	El sistema debe contar con especificaciones técnicas de seguridad para evitar la intrusión de malware.	Preventivo	14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS.	14.1.1	Analista de costos	Jefe de TI
EO-11		Posible error al generar Hoja de Entrada de Servicios debido a la indisponibilidad del sistema originado por falla en el servidor.	Alto	Reducir	Monitorear y hacer seguimiento a las operaciones del servidor.	Preventivo	16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	16.1.5	Analista de costos	Jefe de TI
EO-13		Posible error al generar el número de la Hoja de Entrada de Servicios debido a una falla al cargar la Hoja de Valorización originado por problemas con el sistema.	Alto	Reducir	Realizar regularmente el mantenimiento de los servidores.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES.	12.1.3	Analista de costos	Jefe de TI
EO-16		Posible error al enviar la solicitud de información de costos a cargar debido a una falla en el sistema de correo originado por fallas en el software.	Alto	Reducir	Realizar el mantenimiento preventivo respectivo a los servidores.	Preventivo	11. SEGURIDAD FÍSICA Y DEL ENTORNO.	11.2.4	Gerente de Plaza	Jefe de TI

IDENTIFICACIÓN DE RIESGOS			EVALUACIÓN DE RIESGOS	TRATAMIENTO DE RIESGOS						
Cód. Riesgo	Proceso	Formulación del riesgo	Nivel de riesgo	Estrategia de respuesta	Plan de contingencia	Tipo de control	Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Responsable del proceso	Responsable del control
EO-19	Ejecución de Obra	Posible inexactitud en la información del Perfil de Cierre debido a que no se han registrado todos los costos ejecutados del proyecto originado por el descuido del personal encargado.	Alto	Reducir	Supervisar y monitorear que la información de costos esté disponible.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES.	12.1.3	Gerente de proyecto	Gerente de proyecto
EO-23		Posible falla en el envío del memorándum debido a la indisponibilidad del servicio de correo originado por una falla en el servicio de internet.	Alto	Evitar	Establecer condiciones extras en caso de incumplimiento del servicio	Preventivo	13. SEGURIDAD EN LAS COMUNICACIONES 15. RELACIONES CON PROVEEDORES.	13.1.2 15.2.1	Gerente de Plaza	Gerente de proyecto
EO-24		Posible error en la comunicación con vía correo con el Gerente de PMO debido a una falla en la aplicación de correo originado por una falla del servidor de correos.	Alto	Reducir	Monitorear y hacer seguimiento a las operaciones del servidor.	Preventivo	13. SEGURIDAD EN LAS COMUNICACIONES 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	13.1.2 16.1.5	Gerente de producto	Jefe de TI
EO-26		Posible inexactitud en la información de sustentos de provisiones debido a la falta de documentación originado por la pérdida del mismo.	Alto	Reducir	Establecer políticas de respaldo de información, realizar backups.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES.	12.3.1	Gerente de PMO	Gerente de PMO
EO-28		Posible envío de correo falso indicando conformidad de documentación debido a la intrusión de un malware originado por un hacker.	Alto	Reducir	Establecer políticas de seguridad con respecto al uso de correo electrónico.	Preventivo	13. SEGURIDAD EN LAS COMUNICACIONES 12. SEGURIDAD EN LAS OPERACIONES.	13.2.3 12.2.1	Gerente de PMO	Gerente de PMO
EO-30		Posible error en la elaboración del plano debido al inadecuado seguimiento del servicio originado por el personal responsable.	Alto	Reducir	Establecer condiciones extras en caso de incumplimiento del servicio	Preventivo	15. RELACIONES CON PROVEEDORES.	15.2.1	Gerente de proyecto	Gerente de proyecto
EO-31		Posible pérdida del plano debido a la falla de la aplicación originado por fallas del software.	Alto	Reducir	Establecer políticas de actualización de software, respaldo de información, realizar backups.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES.	12.3.1	Gerente de proyecto	Gerente de proyecto
EO-32		Posible error al enviar el plano para revisión debido a la interrupción de la aplicación de correo originado por falla en el servicio de red.	Alto	Reducir	Monitorear y hacer seguimiento a las operaciones del servidor.	Preventivo	13. SEGURIDAD EN LAS COMUNICACIONES.	13.1.1	Gerente de proyecto	Gerente de proyecto

IDENTIFICACIÓN DE RIESGOS			EVALUACIÓN DE RIESGOS	TRATAMIENTO DE RIESGOS						
Cód. Riesgo	Proceso	Formulación del riesgo	Nivel de riesgo	Estrategia de respuesta	Plan de contingencia	Tipo de control	Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Responsable del proceso	Responsable del control
EO-33	Ejecución de Obra	Posible retraso en la revisión del último plano cargado debido a la indisponibilidad del sistema SGI para mostrarlo originado por falla en el software.	Alto	Reducir	Realizar regularmente el mantenimiento de los servidores.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES.	12.1.3	Jefe de oficina técnica	Jefe de TI
EO-36		Posible error al cargar el plano de obra al sistema debido a la indisponibilidad del servicio originado por falla en el servidor.	Alto	Reducir	Realizar regularmente el mantenimiento de los servidores.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES.	12.1.3	Jefe de oficina técnica	Jefe de TI
EO-37		Posible inexactitud del plano de obra cargado en el sistema debido al error en la comparación de planos originado por el personal encargado.	Alto	Reducir	Realizar capacitaciones continuas al personal.	Preventivo	7. SEGURIDAD EN LOS RECURSOS HUMANOS.	7.2.2	Jefe de oficina técnica	Gerente de proyecto
EO-39		Posible indisponibilidad de los planos por lote debido al retraso en su elaboración originado por el servicio tercerizado.	Alto	Reducir	Establecer condiciones extras en caso de incumplimiento del servicio	Preventivo	15. RELACIONES CON PROVEEDORES.	15.1.1	Jefe de oficina técnica	Gerente de proyecto
VV-01	Ventas	Posible error al cargar las bases de datos de clientes debido a la indisponibilidad del sistema CRM originado por fallo del software.	Alto	Reducir	Monitorear y hacer seguimiento a las operaciones del sistema.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES. 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS.	12.6.1 14.1.2	Ejecutivos de ventas VIP	Gerente de Ventas
VV-02		Posible filtración de la base de clientes debido a la intrusión de un programa malicioso originado por un hacker.	Extremo	Reducir	Establecer políticas de seguridad para cumplir con la ley de protección de datos personales.	Correctivo	12. SEGURIDAD EN LAS OPERACIONES. 18. CUMPLIMIENTO.	12.6.1 18.2.4	Ejecutivos de ventas VIP	Gerente de Ventas
VV-04		Posible entrega de información falsa sobre los productos a los clientes debido a la falta de actualización de los speech por parte del ejecutivo de ventas.	Alto	Evitar	Actualización de los procesos y documentación respectivos.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES.	12.1.1	Ejecutivos de ventas VIP	Gerente de Ventas
VV-05		Posible error al enviar el recibo al cliente debido a la falla del servicio de correo originado por falla en el hardware.	Alto	Reducir	Monitorear y hacer seguimiento a las operaciones del servidor.	Preventivo	12. SEGURIDAD EN LAS OPERACIONES. 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	12.1.3 16.1.5	Ejecutivos de ventas VIP	Jefe de TI
VV-06		Posible error al enviar el recibo al cliente debido a la falla del servicio de correo originado por falla en la red.	Alto	Reducir	Se debe segregar grupos de servicio en las redes.	Preventivo	13. SEGURIDAD EN LAS COMUNICACIONES.	13.1.3	Ejecutivos de ventas VIP	Gerente de Ventas

IDENTIFICACIÓN DE RIESGOS			EVALUACIÓN DE RIESGOS	TRATAMIENTO DE RIESGOS						
Cód. Riesgo	Proceso	Formulación del riesgo	Nivel de riesgo	Estrategia de respuesta	Plan de contingencia	Tipo de control	Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Responsable del proceso	Responsable del control
VV-08	Ventas	Posible error al cargar los datos del cliente al SGI debido a la interrupción del sistema originado por falla en el servicio de red de la caseta.	Alto	Reducir	Colocar más puntos de red de tal manera que el servicio de red esté disponible al 100%	Correctivo	13. SEGURIDAD EN LAS COMUNICACIONES.	13.2.1	Coordinador de ventas	Gerente de Ventas
VV-11		Posible error al cerrar la venta debido a problemas con el SGI originado por falla con el servidor de aplicaciones.	Alto	Reducir	Realizar regularmente el mantenimiento de los servidores.	Preventivo	11. SEGURIDAD FÍSICA Y DEL ENTORNO. 12. SEGURIDAD EN LAS OPERACIONES.	11.2.4 12.1.3	Auxiliar de Créditos y Cobranzas	Jefe de TI
VV-12		Posible filtración de la información de los clientes debido a la intrusión de un malware originado por un hacker.	Extremo	Reducir	Establecer políticas de seguridad para cumplir con la ley de protección de datos personales.	Correctivo	12. SEGURIDAD EN LAS OPERACIONES. 18. CUMPLIMIENTO	12.2.1 18.1.4	Coordinador de ventas	Gerente de Ventas
CC-01	Cobranzas	Posible inconsistencia entre la información registrada en el SGI y en las letras debido al inadecuado registro originado por el personal de venta.	Alto	Evitar	Establecer políticas de escritorios y pantallas limpias en la organización	Preventivo	8. GESTIÓN DE ACTIVOS 11. SEGURIDAD FÍSICA Y DEL ENTORNO.	8.2.3 11.2.9	Asistente de Créditos y Cobranzas	Jefe de CyC
CC-02		Posible extravío de las letras debido al descuido del personal encargado originado por la inadecuado proceso de almacenamiento.	Alto	Evitar	Actualización de los procesos respectivos.	Preventivo	8. GESTIÓN DE ACTIVOS 12. SEGURIDAD EN LAS OPERACIONES.	8.2.3 12.1.1	Asistente de administración de letras	Jefe de CyC
CC-03		Posible extravío de las letras debido al descuido del courier originado por la inadecuado proceso de entrega.	Alto	Reducir	Establecer condiciones extras en caso de incumplimiento del servicio	Preventivo	15. RELACIONES CON PROVEEDORES.	15.1.1	Asistente de administración de letras	Jefe de CyC
CC-06		Posible inconsistencias entre la información de letras registrado por el banco y el SGI debido al inadecuado registro originado por el software.	Alto	Reducir	Asegurarse que la información de las lettras correspondan a las que se registran en el sistema.	Preventivo	13. SEGURIDAD EN LAS COMUNICACIONES.	13.2.1	Supervisor de Créditos y Cobranzas	Jefe de CyC

IDENTIFICACIÓN DE RIESGOS			EVALUACIÓN DE RIESGOS	TRATAMIENTO DE RIESGOS						
Cód. Riesgo	Proceso	Formulación del riesgo	Nivel de riesgo	Estrategia de respuesta	Plan de contingencia	Tipo de control	Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Responsable del proceso	Responsable del control
TI-01	Tecnología de información	Posible error en la asignación de accesos a usuarios debido a la ausencia de una matriz de perfiles en la organización originado por falta de documentación.	Extremo	Reducir	Se debe revisar y actualizar los derechos a accesos de los usuarios.	Detectivo	9. CONTROL DE ACCESOS.	9.2.5	Jefe de TI	Gerente de TI
TI-02		Posible fraude interno debido a la asignación de activos y/o aplicativos a usuarios no autorizados originado por error del personal encargado.	Alto	Evitar	Actualizar lista de perfiles de acceso de la empresa.	Correctivo	7. SEGURIDAD EN LOS RECURSOS HUMANOS. 9. CONTROL DE ACCESOS.	7.2.3 9.4.4	Jefe de TI	Gerente de TI
TI-06		Posible fraude externo debido al acceso no autorizado de un excolaborador que tuvo dos perfiles activos, al cual sólo se desactivaron los accesos de un solo perfil.	Alto	Evitar	Establecer políticas sobre la matriz de perfiles de usuario y gestión de accesos.	Correctivo	9. CONTROL DE ACCESOS.	9.1.1	Jefe de TI	Gerente de TI
TI-07		Posible interrupción o compromiso del servidor de aplicaciones debido a un ataque de denegación de servicio originado por la infección de un troyano.	Alto	Reducir	Monitoreo exhaustivo de los servidores y aplicaciones. Controles contra malware.	Detectivo	12. SEGURIDAD EN LAS OPERACIONES. 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	12.2.1 16.1.2	Jefe de TI	Gerente de TI
TI-08		Posible interrrupción en el funcionamiento de sistemas de información debido a la destrucción o daño de las instalaciones de procesamiento de datos originado por un terremoto en la zona.	Extremo	Reducir	Establecer políticas para la protección física ante desastres naturales.	Preventivo	11. SEGURIDAD FÍSICA Y DEL ENTORNO. 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	11.1.4 16.1.1	Jefe de TI	Gerente de TI
TI-09		Posible alteración de los datos almacenados de forma magnética debido a fallos en el funcionamiento de los equipos de cómputo originado por fallos en el suministro eléctrico.	Alto	Reducir	Realizar capacitaciones continuas al personal sobre seguridad física.	Preventivo	11. SEGURIDAD FÍSICA Y DEL ENTORNO. 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	11.1.3 16.1.1	Jefe de TI	Gerente de TI
TI-10		Posible filtración de información de colaboradores de la organización debido al ataque con un malware originado por un hacker.	Alto	Reducir	Establecer políticas de seguridad para cumplir con la ley de protección de datos personales.	Correctivo	12. SEGURIDAD EN LAS OPERACIONES 18. CUMPLIMIENTO.	12.2.1 18.2.4	Jefe de TI	Gerente de TI

ANEXO F. Declaración de Aplicabilidad

Declaración de Aplicabilidad					
ISO 27001:2013 Controles de Seguridad			**¿Es aplicable a la organización?**		**Justificación de aplicabilidad**
Cláusula	**Sección**	**Objetivo de Control / Control**			
5 Políticas de Seguridad	**5,1**	**Dirección de la Alta Gerencia para la Seguridad de la Información**			
	5.1.1	Políticas de Seguridad de la Información	Aplica	✓	Es necesario el establecimiento de una Política de Seguridad de información, esta servirá de base para iniciar la Gestión de Seguridad de Información.
	5.1.2	Revisión de las Políticas de Seguridad de la Información	Aplica	✓	En la empresa no hay ninguna Política de Seguridad de información actualizada y aprobada. Es necesario que las políticas de Seguridad de Información sean revisadas antes de ser aprobadas.
6 Organización de la Seguridad de la Información	**6,1**	**Organización Interna**			
	6.1.1	Roles y Responsabilidad de Seguridad de la Información	Aplica	✓	No hay roles de Seguridad de información propiamente dichos, los que asumen esa responsabilidad, son los jefes de soporte y el Jefe de infraestructura de TI. Por ello es necesario definir roles de seguridad de información dentro de la organización, para evitar la sobrecarga de actividades.
	6.1.2	Segregación de deberes	Aplica	✓	Actualmente, el rol del Jefe de Soporte de TI está sobrecargado de responsabilidades. Es necesario segregar funciones entre los roles de la organización, de esta manera evitar la sobrecarga de tareas y la ineficiente ejecución de los procesos.
	6.1.3	Contacto con autoridades	No aplica	☒	No hay una entidad que exija a la inmobiliaria a implementar un SGSI.
	6.1.4	Contacto con grupos de interés especial	No aplica	☒	No hay una entidad que exija a la inmobiliaria a implementar un SGSI.
	6.1.5	Seguridad de la Información en la gestión de proyectos	Aplica	✓	En la empresa, no existe una metodología de riesgos definida para poder realizar el análisis de riesgos de seguridad en los proyectos.Es necesario incluir a la seguridad de Información e identificar los controles necesarios en la Gestión de los proyectos.
	6,2	**Dispositivos móviles y teletrabajo**			
	6.2.1	Política de dispositivos móviles	Aplica	✓	No hay documentación actualizada sobre políticas del uso de dispositivos móviles.
	6.2.2	Teletrabajo	Aplica	✓	El negocio de la inmobiliaria hace que el trabajo a distancia o teletrabajo sea muy usado. El trabajo se realiza fuera de las oficinas centrales.
7 Seguridad en los Recursos Humanos	**7,1**	**Previo al Empleo**			
	7.1.1	Verificación de antecedentes	Aplica	✓	En el área de Capital Humano, y como parte del proceso de selección y reclutamiento se revisan los antecedentes penales y policiales de cada uno de los canditatos a un puesto laboral. Sin embargo es necesario realizar una búsqueda o investigación más exhaustiva si el puesto laboral tiene mayor rango.
	7.1.2	Términos y condiciones del empleo	Aplica	✓	Como parte de las cláusulas del contrato firmado por los colaboradores se establece una de confidencialidad hacia la empresa; sin embargo, no se establece la confidencialidad respectiva a los datos personales del trabajador; es por ello que es necesario incluir ciertas cláusulas que cumplan con la ley de Protección de datos Personales.
	7,2	**Durante el Empleo**			
	7.2.1	Responsabilidades de la Alta Gerencia	Aplica	✓	Es necesario hacer que los colaboradores apliquen la seguridad con relación a las políticas y procedimientos de la organización.
	7.2.2	Conciencia, educación y entrenamiento de Seguridad de la Información	Aplica	✓	Actualmente, no se toma en cuenta algunos aspectos de seguridad de información en la cultura organizacional, es por ello que es necesario que todos los colaboradores de la organización deben recibir una adecuada concientización, entrenamiento y actualizaciones regulares en los procesos y políticas organizacionales, como acciones relevantes de su función laboral.
	7.2.3	Proceso disciplinario	Aplica	✓	Es necesario que hayan sanciones para aquellos colaboradores que cometan una violación a la seguridad o que hayan incumplido con la política aprobada.
	7,3	**Terminación y Cambio de Empleo**			
	7.3.1	Termino de responsabilidades o cambio de empleo	Aplica	✓	Una vez que culmine el contrato de un colaborador, las responsabilidades de seguridad de la información y funciones deben seguir vigentes después del término o cambio de empleo. Asimismo, estas responsabilidades deben ser definidas, y comunicas al trabajador o contratista.

ISO 27001:2013 Controles de Seguridad			¿Es aplicable a la organización?		Justificación de aplicabilidad
Cláusula	Sección	Objetivo de Control / Control			
8 Gestión de Activos	8,1	**Responsabilidad de los Activos**			
	8.1.1	Inventario de activos	Aplica	✓	Es necesario realizar un listado de activos de información en la organización, con el fin de hacer seguimiento y monitorearlos. Como parte del diseño del SGSI se ha realizado un inventario de activos de información en los procesos del alcance.
	8.1.2	Propiedad de activos	Aplica	✓	Es necesario realizar un listado de activos de información en la organización, con el fin de hacer seguimiento y monitorearlos. Como parte del diseño del SGSI se ha realizado un inventario de activos de información en los procesos del alcance, asimismo se especifican las propiedades de cada uno.
	8.1.3	Uso aceptable de los activos	Aplica	✓	Si bien en el reglamento interno de trabajo se menciona acerca del adecuado uso de los activos de la empresa, no ha sido difundido correctamente.
	8.1.4	Devolución de activos	Aplica	✓	Se debe definir en un procedimiento, las acividades que se realizan para la devolución de los activos de la organización que están en posesión de algún colaborador cuando termine su contrato.
	8,2	**Clasificación de la Información**			
	8.2.1	Clasificación de la información	Aplica	✓	De acuerdo al inventario de activos de información, se debe clasificar en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización.
	8.2.2	Etiquetado de la información	Aplica	✓	Actualmente no se ha definido un procedimiento para etiquetar o clasificar la información. Asimismo se debe definir un esquema de clasificación de activos para la inmobiliaria.
	8.2.3	Manejo de activos	Aplica	✓	Actualmente no se ha definido un procedimiento para etiquetar o clasificar la información. Asimismo se debe definir un esquema de clasificación de activos para la inmobiliaria.
	8,3	**Manejo de Medios**			
	8.3.1	Gestión de medios removibles	Aplica	✓	El uso de laptop para la venta de productos inmobiliarios fuera de la sede central requiere estos tipo de activos sean protegidos. Si la información es confidencial o debe ser integral necesitará de técnicas criptográficas para protegerla.
	8.3.2	Eliminación de medios	Aplica	✓	El uso de laptop para la venta de productos inmobiliarios fuera de la sede central requiere estos tipo de activos sean protegidos. Si la información es confidencial o debe ser integral necesitará de técnicas criptográficas para protegerla.
	8.3.3	Transporte de medios físicos	Aplica	✓	El uso de laptop para la venta de productos inmobiliarios fuera de la sede central requiere estos tipo de activos sean protegidos. Si la información es confidencial o debe ser integral necesitará de técnicas criptográficas para protegerla.
9 Control de Acceso	9,1	**Requerimientos de Negocio para el Control de Acceso**			
	9.1.1	Política de control de acceso	Aplica	✓	No hay políticas actualizadas con respecto al control de acceso.
	9.1.2	Política en el uso de servicios de red	Aplica	✓	No hay políticas actualizadas con respecto al uso de servicios de red..
	9,2	**Gestión de Accesos de Usuario**			
	9.2.1	Registro y baja del usuario	Aplica	✓	De acuerdo al análisis de riesgo desarrollado, se ha identificado la ausencia de una matriz de perfiles de accceso actualizada, lo que ha ocasionado a que la información se exponga a varios riesgos de seguridad.
	9.2.2	Abastecimiento de usuarios de acceso	Aplica	✓	No hay un procedimiento en el que se abastezcan de usuarios de acceso.
	9.2.3	Gestión de accesos privilegiados	Aplica	✓	Es necesario realizar un procedimiento documentado, en el cual se indique que cada jefe de área, debe solicitar los permisos adecuados para cada colaborador que se le autorice.
	9.2.4	Gestión de información de autenticación secreta de usuarios	Aplica	✓	Es necesario establecer lineamientos para la adecuada gestión de autenticación de usuarios.
	9.2.5	Revisión de derechos de acceso de usuarios	Aplica	✓	De acuerdo al análisis de riesgo desarrollado, se ha identificado la ausencia de una matriz de perfiles de accceso actualizada, lo que ha ocasionado a que la información se exponga a varios riesgos de seguridad.
	9.2.6	Eliminación o ajuste de derechos de acceso	Aplica	✓	De acuerdo al análisis de riesgo desarrollado, se ha identificado la ausencia de una matriz de perfiles de accceso actualizada, lo que ha ocasionado a que la información se exponga a varios riesgos de seguridad.
	9,3	**Responsabilidades del Usuario**			
	9.3.1	Uso de información de autenticación secreta	Aplica	✓	No hay una cultura de seguridad en los colaboradores de la organización, esto hace que las vulnerabilidades se vean expuestas Es por ellos que es necesario que cada trabajador sea responsable de su usuario y contraseña.
	9,4	**Control de Acceso de Sistemas y Aplicaciones**			
	9.4.1	Restricción de acceso a la información	Aplica	✓	Actualmente no hay una comunicación formal con el área de TI acerca de los colaboradores que rota dentro de la empresa, asimismo la ausencia de una matriz de perfiles de accceso actualizada dificulta la ejecución de algunos procesos, por ello es necesario establecer controles de acceso.

ISO 27001:2013 Controles de Seguridad			¿Es aplicable a la organización?		Justificación de aplicabilidad
Cláusula	**Sección**	**Objetivo de Control / Control**			
9 Control de Acceso	9.4.2	Procedimientos de conexión segura	Aplica	✓	Es necesario establecer lineamientos para la establecer una conexión segura al acceder a los sistemas y aplicaciones.
	9.4.3	Sistema de gestión de contraseñas	Aplica	✓	Debe actualizarse el documento en el que tenga las políticas de uso de contraseñas, asimismo debe documentarse las actividades necesarias para la creación de contraseñas a nuevos usuarios, adicionalmente se deberá solicitar a los usuarios que firmen un compromiso para no compartir su contraseña con otros usuarios.
	9.4.4	Uso de programas y utilidades privilegiadas	Aplica	✓	Es necesario realizar un procedimiento documentado, en el cual se indique que cada jefe de área, debe solicitar los permisos adecuados para cada colaborador que se le autorice.
	9.4.5	Control de acceso al código fuente del programa	Aplica	✓	De acuerdo al análisis de riesgo desarrollado, se ha identificado la ausencia de una matriz de perfiles de accceso actualizada, lo que ha ocasionado a que la información se exponga a varios riesgos de seguridad.
10 Criptografía	**10,1**	**Controles Criptográficos**			
	10.1.1	Política en el uso de controles criptográficos	No aplica	☒	En el alcance del SGSI para la inmobiliaria no se incluye esta cláusula.
	10.1.2	Gestión de claves	No aplica	☒	En el alcance del SGSI para la inmobiliaria no se incluye esta cláusula.
11 Seguridad Física y del Entorno	**11,1**	**Áreas Seguras**			
	11.1.1	Perímetro de seguridad físico	Aplica	✓	Se deben establecer controles, políticas en las casetas de ventas de la unidad de vivienda,
	11.1.2	Controles físicos de entrada	Aplica	✓	Se deben establecer controles, políticas en las casetas de ventas de la unidad de vivienda,
	11.1.3	Seguridad de oficinas, habitaciones y facilidades	Aplica	✓	Se deben establecer controles, políticas en las casetas de ventas de la unidad de vivienda,
	11.1.4	Protección contra amenazas externas y del ambiente	Aplica	✓	Establecer políticas para la protección física ante desastres naturales.
	11.1.5	Trabajo en áreas seguras	Aplica	✓	Se deben establecer controles, políticas en las casetas de ventas de la unidad de vivienda,
	11.1.6	Áreas de entrega y carga	Aplica	✓	Se deben establecer controles, políticas en las casetas de ventas de la unidad de vivienda,
	11,2	**Equipo**			
	11.2.1	Instalación y protección de equipo	No aplica	☒	Existen lineamientos y directivas para mantener una infraestructura segura.
	11.2.2	Servicios de soporte	Aplica	✓	Establecer políticas para definir acuerdos de servicio de soporte a las demás áreas.
	11.2.3	Seguridad en el cableado	No aplica	☒	Existen lineamientos y directivas para mantener una infraestructura de red segura.
	11.2.4	Mantenimiento de equipos	Aplica	✓	Es necesario establecer lineamientos para realizar regularmente el mantenimiento de los servidores.
	11.2.5	Retiro de activos	No aplica	☒	Existen políticas que especifican que los equipos, información y otras aplicaciones no deben ser retiradas fuera de la organización, sin previa autorización.
	11.2.6	Seguridad del equipo	No aplica	☒	Existen políticas que especifican que los equipos, información y otras aplicaciones no deben ser utilizar candados de seguridad.
	11.2.7	Eliminación segura o reuso del equipo	No aplica	☒	Existen políticas que especifican que los equipos, información y otras aplicaciones no deben ser retiradas fuera de la organización, sin previa autorización.
	11.2.8	Equipo de usuario desatendido	No aplica	☒	Existen políticas que especifican que los equipos, información y otras aplicaciones no deben ser retiradas fuera de la organización, sin previa autorización.
	11.2.9	Política de escritorio limpio y pantalla limpia	Aplica	✓	Es necesario establecer lineamientos para realizar mantener un escritorio limpio y pantalla limpia.
12 Seguridad en las Operaciones	**12,1**	**Procedimientos Operacionales y Responsabilidades**			
	12.1.1	Documentación de procedimientos operacionales	Aplica	✓	Establecer lineamientos para garantizar que la información esté disponible. Realizar regularmente el mantenimiento de los servidores.
	12.1.2	Gestión de cambios	No aplica	☒	No aplica al alcance del SGSI
	12.1.3	Gestión de la capacidad	Aplica	✓	Establecer lineamientos para garantizar que la información esté disponible. Realizar regularmente el mantenimiento de los servidores.
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	No aplica	☒	No aplica al alcance del SGSI
	12,2	**Protección de Software Malicioso**			
	12.2.1	Controles contra software malicioso	Aplica	✓	Establecer políticas de seguridad con respecto al uso de correo electrónico, respecto a páginas de internet de contenido dudoso.
	12,3	**Respaldo**			
	12.3.1	Respaldo de información	Aplica	✓	Establecer políticas de respaldo de información, realizar backups.

ISO 27001:2013 Controles de Seguridad			¿Es aplicable a la organización?		Justificación de aplicabilidad
Cláusula	**Sección**	**Objetivo de Control / Control**			
12 Seguridad en las Operaciones	**12,4**	**Registro y Monitoreo**			
	12.4.1	Registro de eventos	No aplica	☒	No aplica al alcance del SGSI
	12.4.2	Protección de registros de información	No aplica	☒	No aplica al alcance del SGSI
	12.4.3	Registros de Administrador y Operador	No aplica	☒	No aplica al alcance del SGSI
	12.4.4	Sincronización de relojes	Aplica	✓	Es necesario establecer lineamientos con respecto a la sincronización de reloj para el funcionamiento de los servidores.
	12,5	**Control de Software Operacional**			
	12.5.1	Instalación de software en sistemas operacionales	No aplica	☒	No aplica al alcance del SGSI
	12,6	**Gestión de Vulnerabilidades Técnicas**			
	12.6.1	Gestión de vulnerabilidades técnicas	Aplica	✓	Establecer políticas de seguridad para cumplir con la ley de protección de datos personales.
	12.6.2	Restricciones en la instalación de software	No aplica	☒	Existen políticas de restricción de software para personal no autorizado, sólo el usuario administrador puede instalar aplicaciones en el equipo.
	12,7	**Consideraciones de Auditoria de Sistemas de información**			
	12.7.1	Controles de Auditoría de Sistemas de Información	No aplica	☒	No aplica al alcance del SGSI
13 Seguridad en las Comunicaciones	**13,1**	**Gestión de Seguridad en Red**			
	13.1.1	Controles de red	Aplica	✓	Se debe establecer políticas y segregar grupos de servicio en las redes, para evitar la congestión de las mismas.
	13.1.2	Seguridad de los servicios en red	Aplica	✓	Se debe segregar grupos de servicio en las redes, para evitar la congestión de las mismas.
	13.1.3	Segregación en redes	Aplica	✓	Se debe segregar grupos de servicio en las redes, para evitar la congestión de las mismas.
	13,2	**Transferencia de Información**			
	13.2.1	Políticas y procedimientos para la transferencia de información	Aplica	✓	Es necesario establecer políticas sobre la transferencia de información, así como monitorear y hacer seguimiento a las operaciones del sistema.
	13.2.2	Acuerdos en la transferencia de información	Aplica	✓	Es necesario establecer políticas sobre la transferencia de información, así como monitorear y hacer seguimiento a las operaciones del sistema.
	13.2.3	Mensajería electrónica	Aplica	✓	Es necesario establecer políticas sobre la transferencia de información, así como monitorear y hacer seguimiento a las operaciones del sistema y servidor de correos.
	13.2.4	Acuerdos de confidencialidad o no-revelación	No aplica	☒	Existen políticas de confidencialidad de información en la organización.
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	**14,1**	**Requerimientos de Seguridad de Sistemas de Información**			
	14.1.1	Análisis y especificación de requerimientos de seguridad	Aplica	✓	El sistema debe contar con especificaciones técnicas de seguridad para evitar la intrusión de malware.
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas	Aplica	✓	El sistema debe contar con especificaciones técnicas de seguridad para evitar la intrusión de malware.
	14.1.3	Protección de transacciones de servicios de aplicación	No aplica	☒	En el alcance del SGSI para la inmobiliaria no se ha incluido el desarrollo de sistemas.
	14,2	**Seguridad en el Proceso de Desarrollo y Soporte**			
	14.2.1	Política de desarrollo seguro	No aplica	☒	En el alcance del SGSI para la inmobiliaria no se ha incluido el desarrollo de sistemas.
	14.2.2	Procedimientos de control de cambios	No aplica	☒	En el alcance del SGSI para la inmobiliaria no se ha incluido el desarrollo de sistemas.
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	No aplica	☒	En el alcance del SGSI para la inmobiliaria no se ha incluido el desarrollo de sistemas.
	14.2.4	Restricción de cambios a paquetes de software	No aplica	☒	En el alcance del SGSI para la inmobiliaria no se ha incluido el desarrollo de sistemas.
	14.2.5	Procedimientos de desarrollo de sistemas	No aplica	☒	En el alcance del SGSI para la inmobiliaria no se ha incluido el desarrollo de sistemas.
	14.2.6	Entorno de desarrollo seguro	No aplica	☒	En el alcance del SGSI para la inmobiliaria no se ha incluido el desarrollo de sistemas.
	14.2.7	Desarrollo tercerizado	No aplica	☒	En el alcance del SGSI para la inmobiliaria no se ha incluido el desarrollo de sistemas.
	14.2.8	Pruebas de seguridad del sistema	No aplica	☒	En el alcance del SGSI para la inmobiliaria no se ha incluido el desarrollo de sistemas.
	14.2.9	Pruebas de aceptación del sistema	No aplica	☒	En el alcance del SGSI para la inmobiliaria no se ha incluido el desarrollo de sistemas.
	14,3	**Datos de Prueba**		☒	
	14.3.1	Protección de datos de prueba	No aplica	☒	En el alcance del SGSI para la inmobiliaria no se ha incluido el desarrollo de sistemas.
15 Relaciones con Proveedores	**15,1**	**Seguridad en Relaciones con el Proveedor**			
	15.1.1	Política de Seguridad de la Información para relaciones con proveedores	Aplica	✓	Establecer condiciones en caso de incumplimiento del servicio.
	15.1.2	Atención de tópicos de seguridad dentro de los acuerdos con proveedores	Aplica	✓	Establecer condiciones en caso de incumplimiento del servicio.
	15.1.3	Cadena de suministros de TIC	No aplica	☒	No se ha definido en el alcance.
	15,2	**Gestión de Entrega de Servicios de Proveedor**			
	15.2.1	Monitoreo y revisión de servicios de proveedor	Aplica	✓	Establecer condiciones en caso de incumplimiento del servicio.
	15.2.2	Gestión de cambios a servicios de proveedor	Aplica	✓	Establecer condiciones en caso de incumplimiento del servicio.

ISO 27001:2013 Controles de Seguridad			¿Es aplicable a la organización?		Justificación de aplicabilidad
Cláusula	Sección	Objetivo de Control / Control			
16 Gestión de Incidentes de Seguridad de la Información	16,1	**Gestión de Incidentes de Seguridad de la Información y Mejoras**			
	16.1.1	Responsabilidades y Procedimientos	Aplica	✓	Se debe mantener evidencia de cada incidencia de seguridad, para generar un histórico de eventos o incidentes, que luego se tomará como retroalimentación. Asimismo se deben mantener procesos actualizados.
	16.1.2	Reporte de eventos de Seguridad de la Información	Aplica	✓	Se debe mantener evidencia de cada incidencia de seguridad, para generar un histórico de eventos o incidentes, que luego se tomará como retroalimentación. Asimismo se deben mantener procesos actualizados.
	16.1.3	Reporte de debilidades de Seguridad de la Información	Aplica	✓	Se debe mantener evidencia de cada incidencia de seguridad, para generar un histórico de eventos o incidentes, que luego se tomará como retroalimentación. Asimismo se deben mantener procesos actualizados.
	16.1.4	Valoración y decisión de eventos de Seguridad de la Información	Aplica	✓	Se debe mantener evidencia de cada incidencia de seguridad, para generar un histórico de eventos o incidentes, que luego se tomará como retroalimentación. Asimismo se deben mantener procesos actualizados.
	16.1.5	Respuesta a incidentes de Seguridad de la Información	Aplica	✓	Se ha identificado como control que es necesario monitorear y hacer seguimiento a las operaciones del servidor.
	16.1.6	Aprendizaje de incidentes de Seguridad de la Información	Aplica	✓	Se debe mantener evidencia de cada incidencia de seguridad, para generar un histórico de eventos o incidentes, que luego se tomará como retroalimentación.
	16.1.7	Colección de evidencia	Aplica	✓	Se debe mantener evidencia de cada incidencia de seguridad, para generar un histórico de eventos o incidentes, que luego se tomará como retroalimentación.
17 Aspectos de Seguridad de la Información para la Gestión de Continuidad del Negocio	17,1	**Seguridad de la Información en la Continuidad**			
	17.1.1	Planeación de Seguridad de la Información en la continuidad	No aplica	☒	No se ha definido en el alcance.
	17.1.2	Implementación de Seguridad de la Información en la continuidad	No aplica	☒	No se ha definido en el alcance.
	17.1.3	Verificación, revisión y evaluación de Seguridad de la Información en la continuidad	No aplica	☒	No se ha definido en el alcance.
	17,2	**Redundancias**			
	17.2.1	Disponibilidad de facilidades de procesamiento de	No aplica	☒	No se ha definido en el alcance.
18 Cumplimiento	18,2	**Cumplimiento con Requerimientos Legales y Contractuales**			
	18.2.1	Identificación de legislación aplicable y requerimientos contractuales	Aplica	✓	Establecer políticas de seguridad para cumplir con la ley de protección de datos personales.
	18.2.2	Derechos de propiedad intelectual (IPR)	Aplica	✓	Establecer políticas de seguridad para cumplir con la ley de protección de datos personales.
	18.2.3	Protección de información documentada	Aplica	✓	Establecer políticas de seguridad para cumplir con la protección de documentación clasificada.
	18.2.4	Privacidad y protección de información personal identificable	Aplica	✓	Establecer políticas de seguridad para cumplir con la ley de protección de datos personales.
	18.2.5	Regulación de controles criptográficos	No aplica	☒	No se aplica esta regulación en la inmobiliaria.
	18,1	**Revisiones de Seguridad de la Información**			
	18.1.1	Revisión independiente de Seguridad de la Información	No aplica	☒	No se ha definido en el alcance.
	18.1.2	Cumplimiento con políticas y estándares de seguridad	No aplica	☒	No se ha definido en el alcance.
	18.1.3	Inspección de cumplimiento técnico	No aplica	☒	No se ha definido en el alcance.

ANEXO G. Documentos visados

Jr. Mariscal La Mar (Ex Ugarte y Moscoso) #991
Esquina con Av. del Ejercito – Magdalena
T: (511) 211 4466 // F: (511) 442 9196
www.losportales.com.pe

Los Portales

Lima, 10 de Octubre de 2014

Señor,
Johan Baldeón Medrano
Coordinador de la especialidad de Ingeniería Informática
Pontificia Universidad Católica del Perú

Presente.-

De mi consideración.

Por medio de la presente carta se informa que la empresa tiene conocimiento y expresa su aceptación de brindar las facilidades a la alumna Zully Justino Salinas con código 20072346, para la realización de su proyecto, denominado "Diseño de un Sistema de Gestión de Seguridad de Información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013", para la obtención del título de Ingeniera Informática. A continuación se presenta el detalle de las actividades que se realizará con los respectivos resultados esperados:

Actividades	Resultados esperados
1. Elaborar la documentación exigida por la norma ISO/IEC 27001:2013.	Documentación requerida por la norma ISO/IEC 27001, de acuerdo a los lineamientos específicos en la norma ISO/IEC 27003.
2. Definir el alcance del sistema.	Alcance del sistema bajo enfoque de procesos.
3. Modelar los procesos de negocio del alcance.	Mapa de procesos de negocio.
4. Definir una metodología de gestión de riesgos.	Metodología de Gestión de Riesgos.
5. Definir una metodología para la valorización de activos.	Relación de activos de información más relevantes.
6. Realizar un mapa de riesgos de los procesos del alcance.	Mapa de riesgos.
7. Identificar los controles asociados a los riesgos identificados, empleando la norma ISO/IEC 27002:2013.	Lista de controles según la ISO/IEC 27002:2013.
8. Elaborar el documento de declaración de aplicabilidad.	Documento de declaración de Aplicabilidad

Se expide la presente carta para los fines correspondientes de la tesista.

Atentamente,

JAIME GONZÁLEZ MELLY
Gerente de TI
Los Portales S.A

Mejoramos tu ciudad, mejoramos tu vida

Política de Seguridad de Información

1. Definición:

La política de Seguridad de Información está formada por un conjunto de principios que la organización debe seguir para asegurar la confiabilidad de sus sistemas informáticos. Por sí misma, no constituye una garantía para la seguridad de información, se convertirá en una cuando responda a los intereses y necesidades de la empresa.

Este documento debe seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, tales como cambio en la infraestructura tecnológica, alta rotación de personal, desarrollo de nuevos servicios, entre otros.

Los principales beneficios de la implementación de la política son:

* Contribuir hacer efectiva la gestión del riesgo.
* Priorizar el valor de la información
* Estandarizar los controles y revisiones de los sistemas de información
* Establecer las bases para el desarrollo de estrategias y planes referidos a la seguridad de información.
* Cumplir con los requerimientos regulatorios y legales pertinentes.
* Brindar un entorno de trabajo seguro a los usuarios.

La entidad seguirá los lineamientos de la presente política de seguridad, así mismo se debe tener en cuenta que la seguridad de la información se caracteriza por la preservación de:

a) Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información;
b) Su integridad, asegurando que la información y sus métodos de proceso sean exactos y completos;
c) Su disponibilidad, asegurando que los usuarios tengan acceso a la información y a sus activos asociados cuando lo requieran.

2. Responsabilidad:

Es responsabilidad de la alta dirección conocer y hacer conocer los lineamientos de la Política de Seguridad de la información a todo el personal, de igual manera el personal es responsable de conocer y cumplir la Política de Seguridad de la Información, las normas relacionadas con ésta, los procedimientos y los estándares generales y aquellos específicamente relacionados con su área de competencia.

Dentro de este contexto, se puede diferenciar niveles de responsabilidad a través de las distintas funciones por parte del

- Área de administración:
  - Promover la difusión y apoyo a la seguridad de la información dentro de la organización y coordinar el proceso de administración de la continuidad de las actividades.
  - Tomar conocimiento y apoyar en el monitoreo de los incidentes relativos a la seguridad informática.
  - Aprobar las principales iniciativas para incrementar la seguridad de información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Área de TI:
  - Minimizar la probabilidad de ocurrencia de incidentes a fin de mitigar el riesgo de errores derivados de estos.
  - Cubrir las necesidades de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnologías de las unidades de negocio.
  - Acordar y aprobar metodologías y procesos relativos a la seguridad de información.
  - Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
  - Coordinar las acciones del Comité de Seguridad de la información de impulsar la implementación de la presente política.
  - Monitorear aquellos cambios significativos derivados de los riesgos que afecten a los recursos informáticos.
- Capital Humano:
  - Notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la política de seguridad de la información y de todas las normas, procedimientos y prácticas que de ella surjan.
- Área legal:
  - Verificar el cumplimiento de la presente Política en lo relacionado a la gestión de los contratos, acuerdos u otra documentación de índole legal de la Organización con sus empleadores y terceros.
- Auditoría interna:
  - Desarrollar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, e informar el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta política y por las normas, procedimientos y prácticas que de ella surjan.

3. Política de Seguridad de la Información:

La información y sistemas de información tienen un valor importante para la organización, por lo que se deberá preservar su confidencialidad, integridad y disponibilidad para darle una efectiva protección a la información de manera que se equilibren los gastos utilizados en controles de seguridad de información contra los daños a la organización.

El objetivo de esta política es establecer lineamientos en la administración de la información con el fin de garantizar la seguridad de los sistemas que satisfaga el

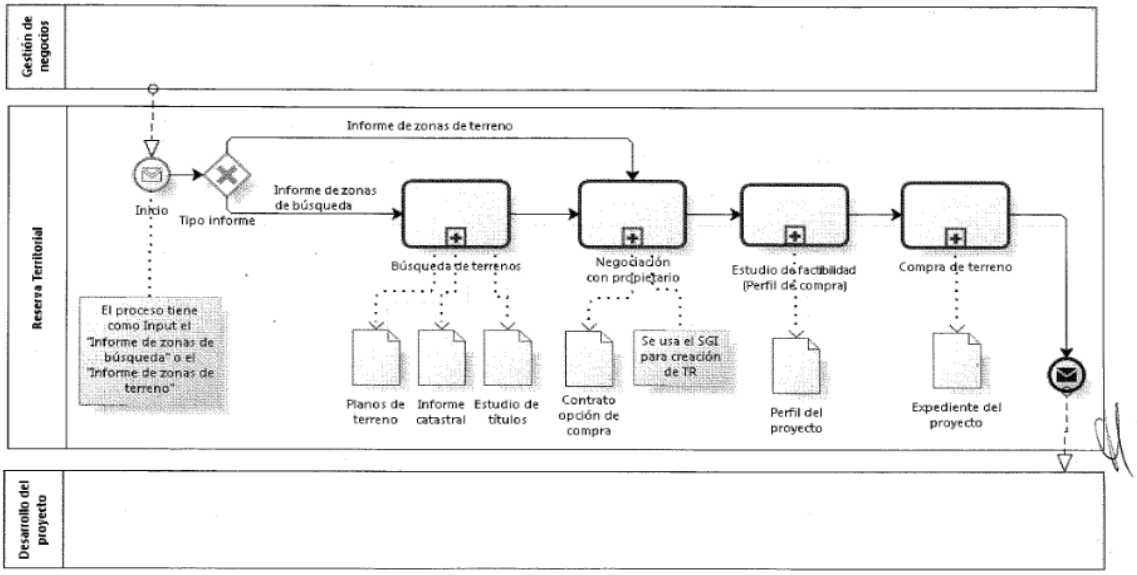
requerimiento del negocio y de mantener la integridad de la información, de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad. De esta manera la empresa se compromete en la formación y sensibilización del personal, contratistas y terceros involucrados, respecto a la seguridad de información para garantizar el cumplimiento de las normativas legales aplicables en busca de la seguridad de la información al interior y fuera de la organización.

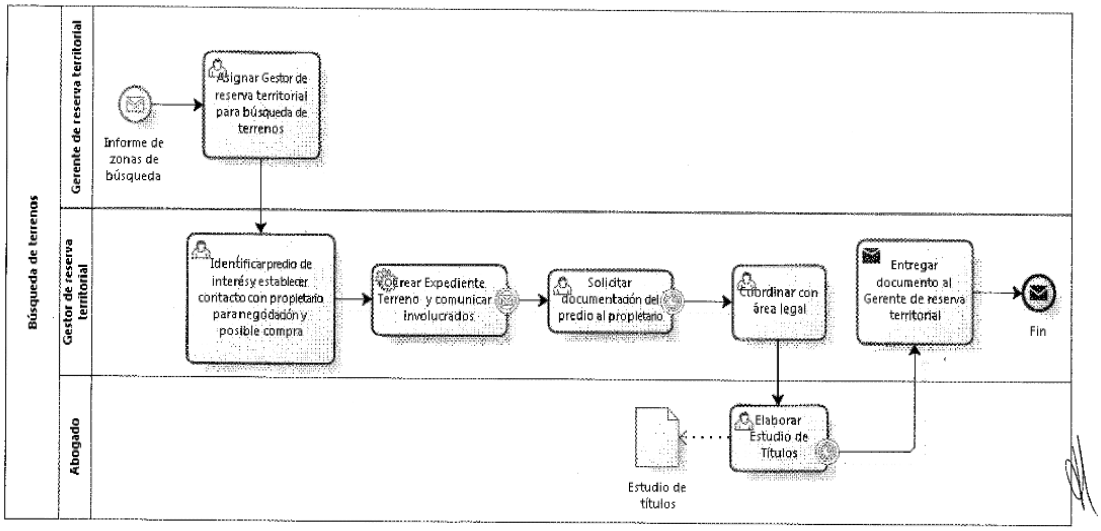
4. Publicación y distribución:

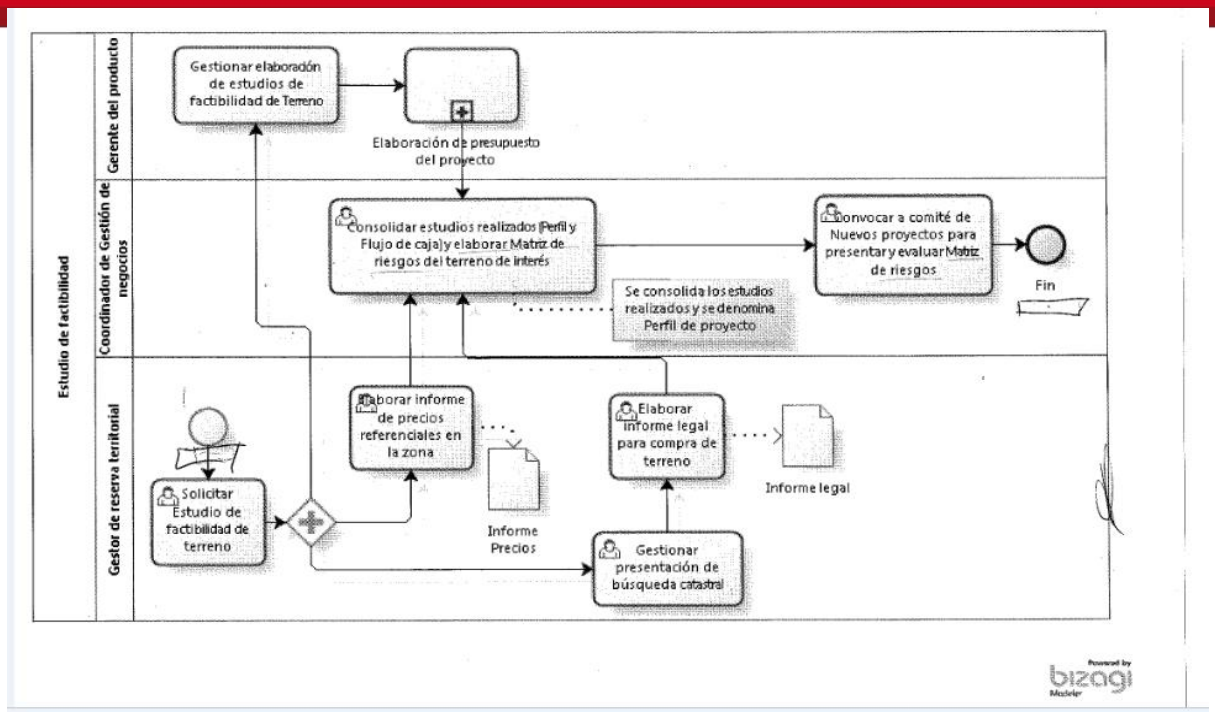
La Política de Seguridad de la información debe ser comunicada a todos los usuarios de la organización, siendo de conocimiento y aplicación obligatorio para todo el personal de la entidad. Por parte de empresa, esta debe publicar y distribuir de forma adecuada hacia todos los niveles de la organización.

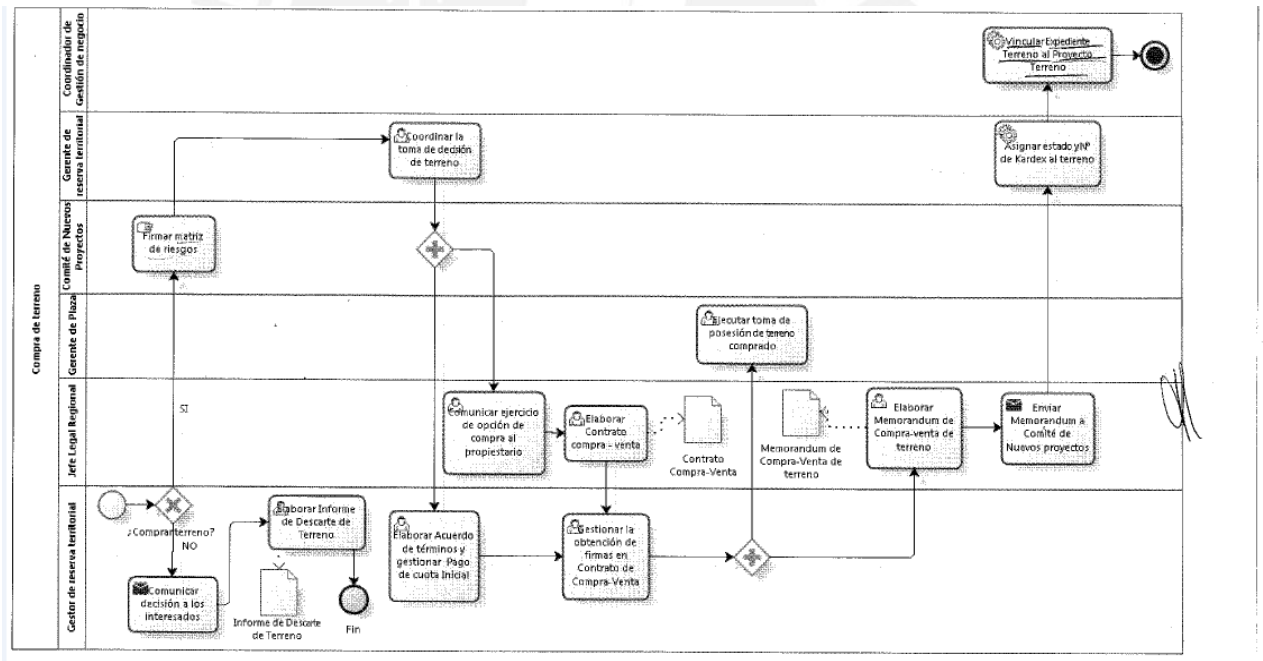
5. Incumplimiento:

A nivel interno, el incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones según el reglamento interno de trabajo (RIT). Las violaciones a la Política de seguridad de información y a cualquier procedimiento o pauta derivados de ésta, que ocasionen cualquier riesgo o pérdida directa para la organización pueden resultar en acción disciplinaria por parte de la organización cuya magnitud depende del tipo y severidad de la violación.


Gestión de negocios
Reserva Territorial
Desarrollo del proyecto
Inicio
Tipo informe
Informe de zonas de terreno
Informe de zonas de búsqueda
Búsqueda de terrenos
Negociación con propietario
Estudio de factibilidad (Perfil de compra)
Compra de terreno
El proceso tiene como Input el "Informe de zonas de búsqueda" o el "Informe de zonas de terreno"
Planos de terreno
Informe catastral
Estudio de títulos
Contrato opción de compra
Se usa el SGI para creación de TR
Perfil del proyecto
Expediente del proyecto


Búsqueda de terrenos
Gerente de reserva territorial
Gestor de reserva territorial
Abogado
Informe de zonas de búsqueda
Asignar Gestor de reserva territorial para búsqueda de terrenos
Identificar predio de interés y establecer contacto con propietario para negociación y posible compra
Crear Expediente Terreno y comunicar involucrados
Solicitar documentación del predio al propietario
Coordinar con área legal
Entregar documento al Gerente de reserva territorial
Fin
Elaborar Estudio de Títulos
Estudio de títulos


Estudio de factibilidad
Gerente del producto
Coordinador de Gestión de negocios
Gestor de reserva territorial
Gestionar elaboradón de estudios de factibilidad de Terreno
Elaboración de presupuesto del proyecto
Consolidar estudios realizados (Perfil y Flujo de caja)y elaborar Matriz de riesgos del terreno de interés
Convocar a comité de Nuevos proyectos para presentary evaluar Matriz de riesgos
Fin
Se consolida los estudios realizados y se denomina Perfil de proyecto
Elaborar informe de precios referenciales en la zona
Elaborar informe legal para compra de terreno
Informe legal
Solicitar Estudio de factibilidad de terreno
Informe Precios
Gestionar presentación de búsqueda catastral
bizagi


Compra de terreno
Coordinador de Gestión de negocio
Gerente de reserva territorial
Comité de Nuevos Proyectos
Gerente de Plaza
Jefe Legal Regional
Gestor de reserva territorial
Vincular Expediente Terreno al Proyecto Terreno
Asignar estado y N° de Kardex al terreno
Coordinar la toma de decisión de terreno
Firmar matriz de riesgos
Ejecutar toma de posesión de terreno comprado
SI
Comunicar ejercicio de opción de compra al propiestario
Elaborar Contrato compra - venta
Contrato Compra-Venta
Memorandum de Compra-Venta de terreno
Elaborar Memorandum de Compra-venta de terreno
Enviar Memorandum a Comité de Nuevos proyectos
¿Comprar terreno?
NO
Elaborar Informe de Descarte de Terreno
Elaborar Acuerdo de términos y gestionar Pago de cuota Inicial
Gestionar la obtención de firmas en Contrato de Compra-Venta
Comunicar decisión a los interesados
Informe de Descarte de Terreno
Fin